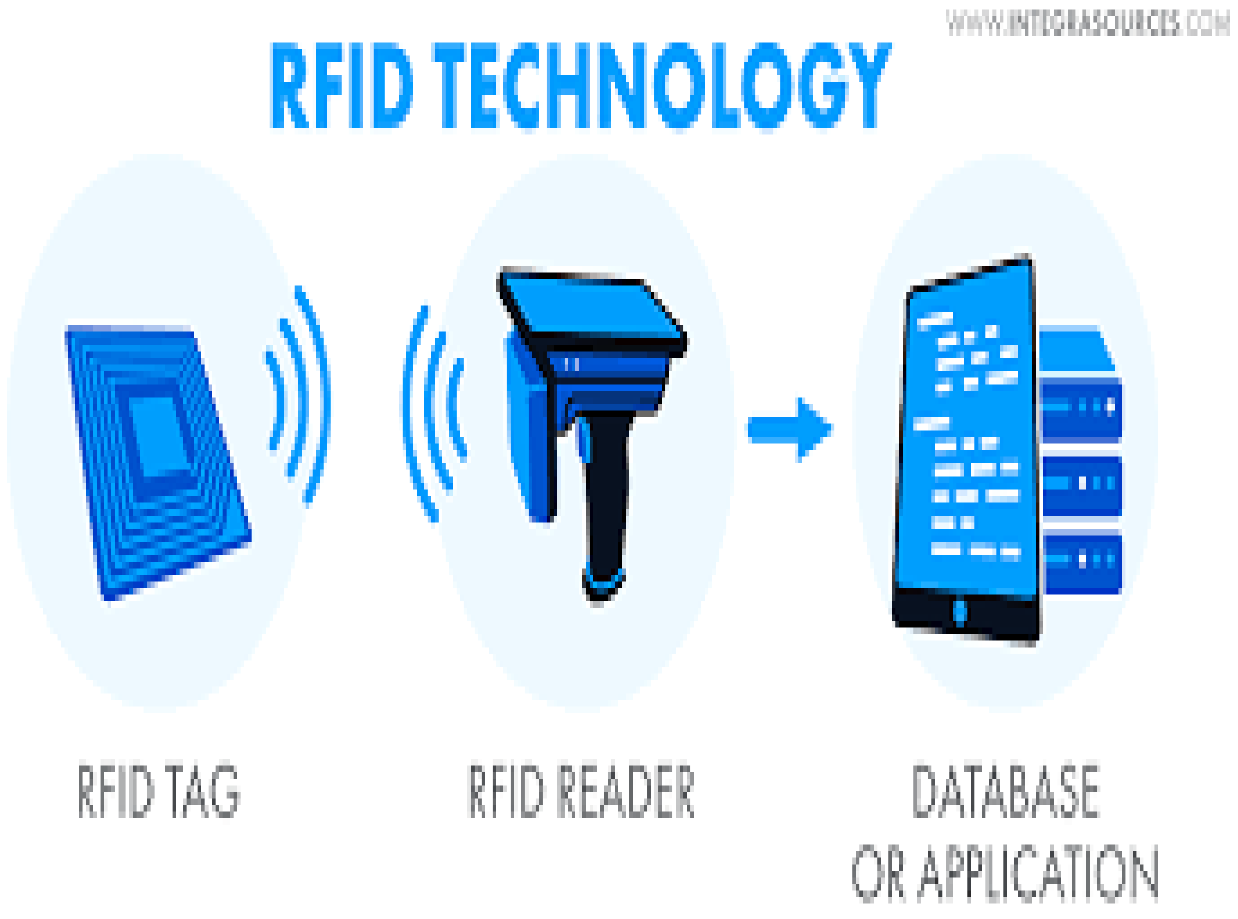
تعلم تغيير رقم رقائق RFID



مقدمة كتاب: تعلم تغيير رقم رقائق RFID: دليل شامل للمبتدئين والمحترفين

في عالم يتسارع فيه التقدم التكنولوجي، أصبحت تقنية **التعرف بموجات الراديو (RFID)** إحدى الركائز الأساسية التي تدعم العديد من الصناعات والتطبيقات اليومية. من بطاقات الدخول التي تفتح أبواب المكاتب، إلى ملصقات التتبع على المنتجات في المتاجر، إلى الرقائق المزروعة في الحيوانات الأليفة لتحديد هويتها، تُعد RFID لغة مشتركة تتحدث بها الأشياء في عالمنا الرقمي. لكن، ماذا لو أردت التحكم بهذه اللغة؟ ماذا لو أردت تعديل أو تغيير المعرف الفريد (UID) أو البيانات المخزنة على رقاقة RFID لتلبية احتياجاتك الخاصة؟ هنا يأتي دور هذا الكتاب، الذي يهدف إلى تمكينك من فهم هذه التقنية الرائعة وإتقان فن تغيير أرقام رقائق RFID بطريقة عملية، آمنة، وقانونية.

لماذا RFID؟

تقنية RFID، أو Radio Frequency Identification، هي نظام يعتمد على موجات الراديو لنقل البيانات بين رقاقة صغيرة (تُسمى Tag أو Transponder) وجهاز قارئ (Reader). تتميز هذه التقنية بقدرتها على تخزين ونقل المعلومات دون الحاجة إلى اتصال مادي أو رؤية مباشرة، مما يجعلها مثالية لتطبيقات متنوعة. على سبيل المثال، عندما تمرر بطاقة الدخول الخاصة بك أمام قارئ الباب، تقوم رقاقة RFID داخل البطاقة بإرسال رقم تعريفي فريد إلى القارئ، الذي يتحقق منه للسماح بالدخول. وفي متجر البيع بالتجزئة، تُستخدم ملصقات RFID لتتبع المنتجات من المستودع إلى الرفوف، مما يقلل من الأخطاء البشرية ويسرّع العمليات.

لكن ما يجعل RFID مثيرة للاهتمام هو مرونتها. في حين أن بعض الرقائق مصممة لتكون للقراءة فقط (Read-Only)، فإن العديد منها قابل لإعادة الكتابة (Read/Write)، مما يتيح لك تعديل البيانات المخزنة عليها، بما في ذلك الأرقام التعريفية أو

المعلومات المخصصة. هذه القدرة تفتح آفاقًا واسعة للابتكار، سواء كنت تدير مخزونًا في شركة، أو تصمم نظام دخول ذكي، أو حتى تستكشف إمكانيات التكنولوجيا كهاوٍ.

لماذا كتاب عن تغيير أرقام RFID؟

تغيير رقم رقاقة RFID ليس مجرد عملية تقنية، بل هو بوابة لفهم كيفية عمل الأنظمة الذكية من حولنا. قد تحتاج إلى تغيير رقم RFID لأسباب عديدة:

- **إدارة المخزون**: لتحديث أرقام المنتجات أو إعادة تخصيص الرقائق في نظام تتبع.
- **التخصيص**: لإنشاء بطاقات دخول مخصصة أو علامات RFID لمشاريع شخصية.
- **إصلاح الأخطاء**: لتصحيح بيانات تم تسجيلها بشكل غير صحيح على الرقاقة.
- **التعلم والاستكشاف**: لفهم كيفية عمل هذه التقنية من خلال التجربة العملية.

ومع ذلك، فإن تغيير أرقام RFID يتطلب معرفة دقيقة بالأدوات، البرمجيات، وهيكلية الرقائق. بدون التوجيه الصحيح، قد تواجه تحديات مثل حماية التشفير، أو عدم توافق الأجهزة، أو حتى مخاطر قانونية إذا تم استخدام التقنية بطريقة غير مسؤولة. هذا الكتاب يهدف إلى سد هذه الفجوة، من خلال تقديم دليل شامل يناسب المبتدئين الذين يتعاملون مع RFID لأول مرة، والمحترفين الذين يبحثون عن تقنيات متقدمة.

ما الذي ستتعلمه من هذا الكتاب؟

هذا الكتاب ليس مجرد مجموعة من التعليمات التقنية، بل هو رحلة تعليمية تأخذك من الأساسيات إلى الإتقان. من خلال فصوله العشرة، ستتعلم:

- **فهم تقنية RFID**: كيف تعمل الرقائق والقارئات، وما هي أنواع الرقائق (LF، HF، UHF) واستخداماتها.
- **استكشاف أرقام RFID**: ما هو المعرف الفريد (UID)، وكيف يتم تنظيم البيانات في القطاعات والكتل.
- **اختيار الأدوات المناسبة**: من قارئات بسيطة مثل ACR122U إلى أجهزة متقدمة مثل Proxmark3، بالإضافة إلى برمجيات مثل NFC Tools وArduino.
- **خطوات تغيير الأرقام**: دليل عملي خطوة بخطوة لقراءة الرقائق، فتح القطاعات المحمية (إذا لزم الأمر)، وكتابة بيانات جديدة.
- **تقنيات متقدمة**: كيفية استخدام Arduino لتخصيص عمليات RFID، بما في ذلك برمجة أنظمة قراءة وكتابة مخصصة.
- **تطبيقات عملية**: كيفية استخدام مهاراتك في إدارة المخزون، أنظمة الدخول، أو حتى المشاريع الإبداعية.
- **الجوانب القانونية والأخلاقية**: كيفية ضمان استخدام التقنية بطريقة مسؤولة ومتوافقة مع القوانين.
- **حل المشكلات**: كيفية التعامل مع الأخطاء الشائعة مثل فشل الكتابة أو مشكلات الاتصال.

من هو جمهور هذا الكتاب؟

تم تصميم هذا الكتاب ليناسب مجموعة واسعة من القراء:

- **المبتدئون**: إذا كنت جديدًا على RFID، فإن الكتاب يبدأ من الصفر، مع شروحات بسيطة وأمثلة عملية. لا تحتاج إلى خلفية تقنية مسبقة، فقط الفضول والرغبة في التعلم.
- **الفنيون والمهندسون**: إذا كنت تعمل في مجال إدارة المخزون، الأمن، أو الإلكترونيات، فإن الكتاب يقدم أدوات وتقنيات متقدمة لتحسين عملك.
- **المتحمسون والهواة**: إذا كنت من عشاق التكنولوجيا أو تحب بناء مشاريعك الخاصة، فإن الكتاب يوفر تمارين ومشاريع إبداعية لاستكشاف إمكانيات RFID.
- **المطورون**: إذا كنت مبرمجًا أو مهتمًا بالبرمجة، فإن قسم Arduino سيمنحك أدوات لبناء حلول RFID مخصصة.

كيف يتميز هذا الكتاب؟

هناك العديد من الموارد التي تتحدث عن RFID، لكن هذا الكتاب يتميز بعدة جوانب:

- **شمولية المحتوى**: يغطي كل شيء من الأساسيات إلى التقنيات المتقدمة، مما يجعله مرجعًا شاملاً.

- **تركيز على التطبيق العملي**: يتضمن تمارين عملية ومشاريع حقيقية تساعدك على تطبيق ما تتعلمه على الفور.
- **صور ومخططات بصرية**: كل فصل مدعوم برسوم توضيحية، مخططات لهيكلية الرقائق، وصور للأدوات، مما يجعل المفاهيم المعقدة سهلة الفهم.
- **تقنيات متقدمة**: يقدم قسمًا خاصًا عن برمجة Arduino، وهو أمر نادر في كتب RFID الموجهة للجمهور العام.
- **نسخة رقمية تفاعلية**: يتضمن الكتاب روابط لفيديوهات توضيحية، أدوات محاكاة، واختبارات تفاعلية، مما يعزز تجربة التعلم.
- **تركيز على الأخلاقيات**: يوجه القراء لاستخدام التقنية بطريقة مسؤولة، مع شرح واضح للجوانب القانونية.

رحلتك مع الكتاب

يبدأ الكتاب بمقدمة نظرية لفهم تقنية RFID ومكوناتها، ثم يأخذك تدريجيًا إلى العمليات العملية. في الفصول الأولى، ستتعلم كيفية اختيار الأدوات المناسبة وإعدادها، بينما تقدم الفصول الوسطى خطوات تغيير الأرقام مع أمثلة واضحة. الفصول المتقدمة تركز على البرمجة والتطبيقات العملية، بينما تنتهي الرحلة بمناقشة المشكلات الشائعة وكيفية حلها، بالإضافة إلى موارد لمواصلة التعلم. كل فصل مدعوم بصور ومخططات توضح الأدوات وهيكلية الرقائق، مع تمارين عملية لتطبيق ما تعلمته. على سبيل المثال، قد يُطلب منك قراءة UID لرقاقة باستخدام تطبيق NFC Tools، أو برمجة Arduino لكتابة بيانات مخصصة. إذا كنت تفضل التعلم المرئي، فإن النسخة الرقمية التفاعلية توفر فيديوهات توضيحية تُظهر الخطوات بوضوح، من توصيل القارئ إلى كتابة الرقم الجديد.

التحديات والفرص

تغيير أرقام RFID ليس بدون تحديات. بعض الرقائق محمية بتشفير قوي، مما يتطلب معرفة بالمفاتيح أو الأذونات. أجهزة القراءة قد تكون معقدة في الإعداد، والأخطاء مثل فشل الكتابة شائعة. لكن هذه التحديات هي جزء من التعلم، وهذا الكتاب مصمم لمساعدتك على التغلب عليها من خلال شروحات مفصلة، أمثلة عملية، وأقسام مخصصة لاستكشاف الأخطاء وإصلاحها.
في الوقت نفسه، فإن إتقان هذه المهارة يفتح أبوابًا للفرص. يمكنك تحسين كفاءة الأعمال من خلال أنظمة تتبع أفضل، أو بناء مشاريع إبداعية مثل أقفال ذكية تعمل بـ RFID، أو حتى المساهمة في مجتمع التكنولوجيا من خلال مشاركة خبراتك. سواء كنت مبتدئًا أو محترفًا، فإن هذا الكتاب سيزودك بالأدوات والثقة للنجاح.

كلمة أخيرة

تقنية RFID هي جسر بين العالم المادي والرقمي، وتغيير أرقام الرقائق هو مفتاح لفتح إمكانياتها. هذا الكتاب هو دليلك للسير في هذا المسار، سواء كنت تسعى لتحسين عملك، استكشاف التكنولوجيا، أو بناء شيء جديد. مع الشروحات البسيطة، الصور التوضيحية، التمارين العملية، والموارد التفاعلية، ستجد نفسك مجهزًا لإتقان هذا المجال بسهولة وثقة. انضم إلينا في هذه الرحلة، واكتشف كيف يمكن لتقنية صغيرة أن تحدث فرقًا كبيرًا.

1.1 ما هي تقنية RFID؟

تقنية **التعرف بموجات الراديو (Radio Frequency Identification - RFID)** هي نظام يستخدم موجات الراديو لنقل البيانات بين رقاقة إلكترونية صغيرة (تُسمى Tag أو Transponder) وجهاز قارئ (Reader). تُعد RFID واحدة من أكثر التقنيات شيوعًا في العالم اليوم، حيث تُستخدم في تطبيقات متنوعة مثل إدارة المخزون، التحكم بالوصول، تتبع الأصول، وحتى تحديد هوية الحيوانات الأليفة.
تعتمد RFID على فكرة بسيطة: الرقاقة تخزن بيانات (مثل رقم تعريفي فريد أو معلومات مخصصة)، وعندما تكون بالقرب من قارئ، ترسل هذه البيانات عبر موجات الراديو. لا تحتاج RFID إلى اتصال مادي أو رؤية مباشرة (مثل الباركود)، مما يجعلها مرنة وفعالة.

تاريخ موجز:

- ظهرت فكرة RFID في أوائل القرن العشرين خلال الحرب العالمية الثانية، حيث استُخدمت لتحديد الطائرات (نظام IFF).

- في السبعينيات، بدأ استخدام RFID في تطبيقات تجارية مثل تتبع الماشية.
- اليوم، أصبحت RFID جزءًا لا يتجزأ من الصناعات، مع رقائق متطورة تدعم التشفير والتخزين الكبير.

1.2 مكونات نظام RFID

يتكون نظام RFID من ثلاثة مكونات رئيسية:

- **الرقاقة (Tag)**:
  - جهاز صغير يحتوي على دائرة إلكترونية وهوائي.
  - تخزن بيانات مثل المعرف الفريد (UID) أو معلومات مخصصة.
  - أنواع الرقائق:
    - **نشطة (Active)**: تحتوي على بطارية، مما يتيح نطاق قراءة أكبر (حتى 100 متر).
    - **سلبية (Passive)**: تعمل بدون بطارية، تعتمد على طاقة القارئ (نطاق 1-10 أمتار).
- **القارئ (Reader)**:
  - جهاز يرسل موجات راديو لتنشيط الرقاقة وقراءة بياناتها.
  - قد يكون محمولًا (مثل قارئ USB) أو ثابتًا (مثل بوابات المتاجر).
- **البرمجيات**:
  - تُستخدم لمعالجة البيانات المقروءة، مثل تسجيلها في قاعدة بيانات أو عرضها على شاشة.
  - أمثلة: NFC Tools، برامج إدارة المخزون.

مخطط تدفق RFID (يُضاف كرسم توضيحي):

[رقاقة RFID] <--- موجات راديو ---> [قارئ USB ---> [RFID/شبكة ---> [برمجيات/قاعدة بيانات]

1. القارئ يرسل إشارة.
2. الرقاقة تستجيب بالبيانات.
3. البرمجيات تعالج البيانات.

ملاحظة: سيتم تضمين مخطط ملون في الكتاب يوضح هذا التدفق، مع أيقونات للرقاقة (مثل ملصق دائري)، القارئ (جهاز بمؤشر LED)، والبرمجيات (شاشة كمبيوتر).

1.3 أنواع رقائق RFID

تُصنف رقائق RFID بناءً على التردد الذي تعمل به، وكل نوع له استخدامات محددة:

- **التردد المنخفض (Low Frequency - LF، 125-134 كيلوهرتز)**:
  - نطاق قراءة قصير (حتى 1 متر).
  - استخدامات: رقائق الحيوانات، بطاقات الدخول البسيطة.
  - مثال: رقاقة مزروعة في كلب لتحديد هويته.
- **التردد العالي (High Frequency - HF، 13.56 ميجاهرتز)**:
  - نطاق متوسط (حتى 1.5 متر).
  - استخدامات: بطاقات NFC، تذاكر النقل العام، بطاقات المكتبات.

- مثال: بطاقة MIFARE Classic المستخدمة في مترو الأنفاق.
- **التردد فوق العالي (Ultra-High Frequency - UHF، 860-960 ميجاهرتز)**:
  - نطاق طويل (حتى 15 مترًا).
  - استخدامات: تتبع المخزون، إدارة اللوجستيات.
  - مثال: ملصقات RFID على المنتجات في المتاجر.

رسم توضيحي (يُضاف في الكتاب):

- جدول بصري يقارن بين LF، HF، UHF من حيث التردد، النطاق، والاستخدامات.
- صورة توضيحية تُظهر أمثلة لكل نوع (رقاقة حيوان، بطاقة NFC، ملصق UHF).

1.4 الفرق بين الرقائق القابلة للكتابة والقراءة فقط

- **رقائق القراءة فقط (Read-Only)**:
  - تحتوي على بيانات ثابتة (مثل UID) لا يمكن تغييرها.
  - تُستخدم في تطبيقات تتطلب أمانًا عاليًا أو بيانات دائمة.
  - مثال: بعض رقائق الحيوانات التي تحمل رقمًا فريدًا.
- **رقائق القراءة/الكتابة (Read/Write)**:
  - تتيح تعديل البيانات المخزنة (مثل UID أو بيانات القطاعات).
  - تُستخدم في تطبيقات مرنة مثل إدارة المخزون أو بطاقات الدخول القابلة لإعادة البرمجة.
  - مثال: بطاقة MIFARE Classic يمكن كتابة أرقام جديدة عليها.

رسوم متحركة (يُضاف في النسخة الرقمية):

- رسم متحرك مدته 30 ثانية يوضح كيف ترسل الرقاقة بياناتها إلى القارئ:
  - المشهد 1: قارئ يُرسل موجات راديو (تمثل بخطوط متموجة).
  - المشهد 2: رقاقة تُضيء وترسل UID (يظهر الرقم على الشاشة).
  - المشهد 3: البرمجيات تعرض البيانات (مثل "UID: A1B2C3D4").
- سيتم إنتاج هذا الرسم باستخدام أدوات مثل Adobe After Effects وإدراجه في النسخة الرقمية.

1.5 استخدامات RFID في الحياة اليومية

تقنية RFID موجودة من حولنا، وغالبًا لا نلاحظها. إليك بعض الأمثلة:

- **التحكم بالوصول**: بطاقات الدخول للمباني أو الفنادق.
- **إدارة المخزون**: ملصقات RFID على المنتجات في المتاجر مثل Zara أو Amazon.
- **النقل العام**: بطاقات NFC في المترو أو الحافلات.
- **تتبع الحيوانات**: رقائق مزروعة في الحيوانات الأليفة لتحديد هويتها.
- **الرعاية الصحية**: أساور RFID لتتبع المرضى أو الأدوية.
- **الفعاليات**: أساور RFID في الحفلات أو المهرجانات للدخول أو الدفع.

صورة توضيحية (يُضاف في الكتاب):

- لوحة بصرية تُظهر 5 تطبيقات (بطاقة دخول، ملصق مخزون، أسورة مستشفى، إلخ) مع وصف مختصر لكل تطبيق.

1.6 لماذا تغيير أرقام RFID؟

تغيير رقم أو بيانات رقاقة RFID قد يكون ضروريًا لأسباب عديدة:

- **إعادة تخصيص الرقائق**: تغيير أرقام لتتبع منتجات جديدة في المخزون.
- **إصلاح الأخطاء**: تصحيح بيانات تم تسجيلها بشكل غير صحيح.
- **التخصيص**: إنشاء بطاقات دخول مخصصة أو علامات لمشاريع شخصية.
- **التعلم**: فهم كيفية عمل الرقائق من خلال التجربة العملية.

ومع ذلك، يتطلب تغيير الأرقام معرفة بالأدوات، البرمجيات، وهيكلية الرقائق، بالإضافة إلى الالتزام بالجوانب القانونية والأخلاقية. هذا الفصل يضع الأساس لهذه الرحلة، بينما تقدم الفصول اللاحقة التفاصيل العملية.

1.7 كيف تعمل RFID؟ (فيديو توضيحي)

فيديو: "كيف تعمل RFID؟"

- **المدة**: 3 دقائق.
- **المحتوى**:
  - **المقدمة (30 ثانية)**: شرح موجز لـ RFID وأهميتها (مع لقطات لبطاقات دخول وملصقات مخزون).
  - **آلية العمل (1.5 دقيقة)**: رسوم متحركة توضح:
    - القارئ يرسل موجات راديو.
    - الرقاقة تستجيب بالبيانات (يظهر UID على شاشة).
    - البرمجيات تعالج البيانات (مثل فتح باب أو تسجيل منتج).
  - **الأمثلة (1 دقيقة)**: لقطات واقعية لاستخدام RFID (مثل تمرير بطاقة مترو، قراءة ملصق في متجر).
- **الإنتاج**:
  - سيتم إنتاج الفيديو باستخدام Adobe Premiere وAfter Effects.
  - تعليق صوتي عربي واضح، مع ترجمات إنجليزية اختيارية.
  - سيتم استضافة الفيديو على يوتيوب مع رابط في الكتاب: youtube.com/rfid-how-it-works (#).
- **دمج في الكتاب**:
  - رمز QR في نهاية الفصل ينقل القارئ إلى الفيديو.
  - وصف مختصر: "شاهد فيديو 'كيف تعمل RFID؟' لفهم الآلية بصريًا."

1.8 تمرين عملي: تحديد استخدامات RFID في الحياة اليومية

الهدف: مساعدة القارئ على ربط المفاهيم النظرية بالحياة الواقعية. **الأدوات المطلوبة**: قلم وورقة، أو جهاز ذكي لتدوين الملاحظات. **الخطوات**:

- فكر في يومك العادي، من الصباح إلى المساء.
- حدد 3 حالات على الأقل تُستخدم فيها RFID (مثل بطاقة دخول، دفع عبر NFC، ملصقات في متجر).
- لكل حالة، اكتب:
  - الاستخدام (مثل "فتح باب المكتب").
  - نوع الرقاقة المحتمل (LF، HF، UHF) بناءً على وصف الفصل.
  - كيف يمكن أن يفيد تغيير رقم الرقاقة في هذا السياق (مثل إعادة برمجة بطاقة دخول لموظف جديد).
- إذا أمكن، التقط صورة لإحدى الحالات (مثل بطاقة مترو) وأضفها إلى ملاحظاتك. **معايير النجاح**:
- تحديد 3 حالات على الأقل مع وصف واضح.
- ربط كل حالة بنوع الرقاقة والفائدة المحتملة لتغيير الرقم. **تحدي إضافي**:
- ابحث عبر الإنترنت عن تطبيق RFID مبتكر (مثل RFID في الملابس الذكية) واشرح كيف يعمل في فقرة قصيرة.

مثال للإجابة:

- **الحالة 1**:

- الاستخدام: بطاقة دخول للجامعة.
- النوع: HF (ربما MIFARE Classic).
- الفائدة: تغيير الرقم لتخصيص البطاقة لطالب جديد.
- **الحالة 2**:
  - الاستخدام: ملصق RFID على منتج في سوبرماركت.
  - النوع: UHF (لنطاق القراءة الطويل).
  - الفائدة: تحديث الرقم لتتبع دفعة جديدة من المنتجات.
- **الحالة 3**:
  - الاستخدام: دفع عبر NFC في هاتف ذكي.
  - النوع: HF (NFC).
  - الفائدة: إعادة برمجة بيانات لتطبيق دفع مخصص.

1.9 ملخص الفصل

- RFID هي تقنية تعتمد على موجات الراديو لنقل البيانات بين الرقائق والقارئات.
- تتكون من رقائق (نشطة أو سلبية)، قارئات، وبرمجيات.
- أنواع الرقائق تشمل LF، HF، وUHF، ولكل منها استخدامات محددة.
- الرقائق قد تكون للقراءة فقط أو قابلة للكتابة، وهذا الفصل ركز على الأساس لفهم كيفية تغيير أرقام الرقائق القابلة للكتابة.
- شاهد فيديو "كيف تعمل RFID؟" وأكمل التمرين العملي لربط المفاهيم بالواقع.

1.10 أسئلة مراجعة

- ما الفرق بين الرقائق النشطة والسلبية؟
- اذكر مثالًا لاستخدام RFID في كل من الترددات: LF، HF، UHF.
- لماذا قد تحتاج إلى تغيير رقم رقاقة RFID؟
- كيف يساعد مخطط تدفق RFID في فهم التقنية؟

1.11 موارد إضافية

- **فيديو**: "كيف تعمل RFID؟" (رابط: youtube.com/rfid-how-it-works (#)).
- **موقع ويب**: RFID Journal (rfidjournal.com) لمزيد من الأخبار والتطبيقات.
- **تطبيق**: قم بتنزيل RFID TagInfo لتجربة قراءة رقاقة إذا كان لديك هاتف يدعم NFC.

1.1 ما هي تقنية RFID؟

تقنية **التعرف بموجات الراديو (RFID)** هي نظام يستخدم موجات الراديو لنقل البيانات بين رقاقة إلكترونية (Tag) وجهاز قارئ (Reader). تُستخدم RFID في تطبيقات متنوعة مثل بطاقات الدخول، تتبع المخزون، وتحديد هوية الحيوانات. تعتمد على نقل البيانات دون الحاجة إلى اتصال مادي أو رؤية مباشرة، مما يجعلها فعالة ومرنة.

1.2 تاريخ RFID: رحلة التطور (قسم جديد)

لتقدير أهمية RFID، من الضروري فهم تطورها عبر الزمن. فيما يلي نظرة مفصلة على تاريخ هذه التقنية:

- **الأربعينيات: النشأة**:
  - خلال الحرب العالمية الثانية، طوّرت تقنيات مبكرة للتعرف على الطائرات باستخدام نظام **IFF (Identify Friend or Foe)**، الذي اعتمد على إشارات راديو لتمييز الطائرات الحليفة عن العدو. يُعتبر هذا النظام الجد الأول لـ RFID.

- **الستينيات-السبعينيات: التطبيقات التجارية الأولى:**
  - في الستينيات، بدأت الأبحاث حول استخدام RFID في تتبع الأغراض. أول تطبيق تجاري كبير كان في تتبع الماشية، حيث استُخدمت رقائق RFID لتسجيل أرقام تعريفية للحيوانات.
  - في عام 1973، طوّر ماريو كاردولو أول براءة اختراع لنظام RFID سلبي يعمل بموجات الراديو.
- **الثمانينيات: الانتشار الصناعي:**
  - بدأت الشركات في استخدام RFID لتتبع الأصول في المصانع والمستودعات. ظهرت رقائق LF (125-134 كيلوهرتز) كخيار شائع بسبب تكلفتها المنخفضة.
- **التسعينيات: التوسع في الترددات:**
  - ظهرت رقائق HF (13.56 ميجاهرتز) مثل MIFARE، مما أتاح تطبيقات مثل بطاقات الدخول وتذاكر النقل العام.
  - بدأ استخدام RFID في سلاسل التوريد، خاصة مع رقائق UHF التي توفر نطاق قراءة أطول.
- **الألفية الجديدة: التكامل مع التكنولوجيا الحديثة:**
  - أصبحت RFID جزءًا من إنترنت الأشياء (IoT)، حيث تُستخدم لتتبع الأغراض في الوقت الفعلي.
  - ظهرت تقنية NFC (جزء من HF RFID) في الهواتف الذكية، مما جعل RFID متاحة للجميع.
- **اليوم (2025):**
  - تُستخدم RFID في المدن الذكية، الرعاية الصحية (مثل أساور المرضى)، والتجارة الإلكترونية.
  - تطورت الرقائق لتدعم التشفير المتقدم (مثل MIFARE DESFire) وسعات تخزين أكبر.

مخطط زمني (يُضاف في الكتاب):

- رسم بصري يُظهر المراحل الرئيسية (1940s: IFF → 1970s: تتبع الماشية → 2000s: NFC → 2025: المدن الذكية).
- سيتم تصميمه بلونين (أزرق للتاريخ، أخضر للتطبيقات) مع أيقونات (طائرة، بقرة، هاتف ذكي).

1.3 مكونات نظام RFID

يتكون نظام RFID من:

- **الرقاقة (Tag)**: تخزن البيانات (مثل UID أو بيانات مخصصة). قد تكون نشطة (ببطارية) أو سلبية (بدون بطارية).
- **القارئ (Reader)**: يرسل موجات راديو لقراءة أو كتابة البيانات.
- **البرمجيات**: تعالج البيانات، مثل عرضها أو تخزينها في قاعدة بيانات.

مخطط تدفق RFID (مُضاف سابقًا):

[رقاقة RFID] <--- موجات راديو ---> [قارئ USB ---> [RFID/شبكة ---> [برمجيات/قاعدة بيانات]

- سيتم تضمين صورة ملونة في الكتاب تُظهر الرقاقة (ملصق دائري)، القارئ (جهاز بمؤشر LED)، والبرمجيات (شاشة كمبيوتر).

1.4 أنواع رقائق RFID

- **التردد المنخفض (LF، 125-134 كيلوهرتز):**
  - نطاق قصير (حتى 1 متر).
  - استخدامات: رقائق الحيوانات، بطاقات الدخول.
- **التردد العالي (HF، 13.56 ميجاهرتز):**

- نطاق متوسط (حتى 1.5 متر).
- استخدامات: بطاقات NFC، تذاكر النقل.
- **التردد فوق العالي (UHF، 860-960 ميجاهرتز)**:
  - نطاق طويل (حتى 15 مترًا).
  - استخدامات: تتبع المخزون، اللوجستيات.

مخطط إضافي: هيكلية رقاقة MIFARE Classic:

- **الوصف**:
  - رقاقة MIFARE Classic (HF) شائعة في بطاقات الدخول والنقل.
  - تحتوي على 16 قطاعًا (Sectors)، كل قطاع يحتوي على 4 كتل (Blocks).
  - القطاع 0، الكتلة 0: تحتوي على UID (غالبًا غير قابل للتعديل). Jonah Hill.
  - الكتل الأخرى: بيانات قابلة للكتابة.
  - القطاع 15: يحتوي على مفاتيح التشفير (Key A وKey B).
- **رسم بصري** (يُضاف في الكتاب):

[Sector 0]
Block 0: UID | Manufacturer Data
Block 1: Data
Block 2: Data
Block 3: Key A | Access Bits | Key B
[Sector 1]
Block 4: Data
Block 5: Data
Block 6: Data
Block 7: Key A | Access Bits | Key B
...

- [Sector 15]
  - سيتم تصميم مخطط ملون يُظهر القطاعات كصناديق مرقمة، مع تلوين مختلف للـ UID (أحمر، غير قابل للتعديل)، البيانات (أخضر، قابل للكتابة)، والمفاتيح (أزرق، محمية).
  - تعليقات توضيحية: "UID: معرف فريد"، "Data: بيانات مخصصة"، "Keys: للتحكم بالوصول".

1.5 الفرق بين الرقائق القابلة للكتابة والقراءة فقط

- **رقائق القراءة فقط**: بيانات ثابتة (مثل UID في بعض رقائق الحيوانات).
- **رقائق القراءة/الكتابة**: تتيح تعديل البيانات (مثل MIFARE Classic).

1.6 استخدامات RFID في الحياة اليومية

- التحكم بالوصول: بطاقات المكاتب.
- إدارة المخزون: ملصقات في المتاجر.
- النقل العام: بطاقات NFC.
- تتبع الحيوانات: رقائق مزروعة.

- الرعاية الصحية: أساور المرضى.

صورة توضيحية:
- لوحة بصرية تُظهر 5 تطبيقات مع صور (بطاقة دخول، ملصق مخزون، أسورة مستشفى).

1.7 دراسة حالة: RFID في إدارة المخزون لدى Zara *(قسم جديد)*

الخلفية:
- Zara، إحدى أكبر شركات الأزياء في العالم، تستخدم RFID لتحسين إدارة المخزون.
- منذ عام 2014، بدأت Zara بإضافة ملصقات RFID (UHF) إلى جميع منتجاتها.

كيف يعمل النظام:
- كل ملصق RFID يحتوي على رقم تعريفي فريد يرتبط بمنتج معين (مثل قميص أزرق، مقاس M).
- القارئات المحمولة تُستخدم في المتاجر لفحص المخزون بسرعة (حتى 25,000 عنصر في الساعة).
- البيانات تُرسل إلى نظام مركزي يحدد المنتجات التي تحتاج إلى إعادة تعبئة.

الفوائد:
- تقليل الأخطاء البشرية في عد المخزون.
- تحسين سرعة إعادة التخزين (من المستودع إلى الرفوف).
- تعزيز تجربة العملاء من خلال توفير المنتجات المطلوبة بسرعة.

تغيير الأرقام:
- في بعض الحالات، قد تُعاد برمجة ملصقات RFID لتتبع دفعات جديدة أو تصحيح أخطاء في تخصيص الأرقام.

رسم توضيحي (يُضاف في الكتاب):
- صورة تُظهر ملصق RFID على قميص Zara، مع قارئ محمول يفحص المخزون.
- مخطط بسيط: [ملصق RFID] → [قارئ محمول] → [نظام المخزون].

أسئلة للتفكير:
- كيف يمكن أن يساعد تغيير أرقام RFID في تحسين نظام Zara؟
- ما نوع الرقائق المستخدمة (LF، HF، UHF) ولماذا؟

1.8 لماذا تغيير أرقام RFID؟

- إعادة تخصيص الرقائق.
- إصلاح الأخطاء.
- التخصيص.
- التعلم والاستكشاف.

1.9 كيف تعمل RFID؟ (فيديو توضيحي)

فيديو: "كيف تعمل RFID؟"

- **المدة**: 3 دقائق.
- **المحتوى**:
  - مقدمة: أهمية RFID.
  - آلية العمل: رسوم متحركة (القارئ يرسل إشارة، الرقاقة تستجيب، البرمجيات تعالج).
  - أمثلة: بطاقة مترو، ملصق متجر.
- **الإنتاج**: Adobe Premiere/After Effects، تعليق صوتي عربي، ترجمات إنجليزية.
- **الدمج**: رمز QR ورابط: youtube.com/rfid-how-it-works (#).

رسوم متحركة:

- رسم متحرك (30 ثانية) يُظهر تدفق البيانات (رقاقة تُضيء، UID يظهر على شاشة).
- مدمج في النسخة الرقمية.

1.10 تمرين عملي: تحديد استخدامات RFID في زيارة متجر (*تمرين أكثر تعقيدًا*)

الهدف: ربط مفاهيم RFID بالتجربة الواقعية من خلال زيارة متجر. **الأدوات المطلوبة**:

- هاتف ذكي (يفضل مع NFC).
- تطبيق RFID TagInfo أو NFC Tools (اختياري).
- دفتر ملاحظات أو تطبيق تدوين. **الخطوات**:
- قم بزيارة متجر بيع بالتجزئة (مثل سوبرماركت، متجر ملابس، أو إلكترونيات).
- ابحث عن علامات RFID المحتملة:
  - تحقق من المنتجات (هل تحتوي على ملصقات إلكترونية؟).
  - لاحظ أي قارئات RFID (مثل بوابات عند المدخل أو أجهزة فحص المخزون).
  - إذا كان لديك هاتف NFC، حاول قراءة ملصق RFID (مثل ملصق على منتج) باستخدام تطبيق RFID TagInfo.
- سجل ملاحظاتك:
  - وصف الحالة (مثل "ملصق RFID على سترة في متجر ملابس").
  - نوع الرقاقة المحتمل (LF، HF، UHF) وسبب اختيارك (مثل "UHF لأن المتجر يستخدم تتبع المخزون بعيد المدى").
  - كيف يمكن أن يفيد تغيير الرقم؟ (مثل "تحديث الرقم لتتبع دفعة جديدة").
  - إذا قرأت رقاقة، دوّن البيانات المعروضة (مثل UID أو نوع الرقاقة).
- التقط صورة (إن أمكن) لملصق RFID أو قارئ في المتجر.
- اكتب فقرة (100 كلمة) تلخص تجربتك، مع الإجابة على:
  - ما نوع نظام RFID المستخدم في المتجر؟
  - كيف يعزز الكفاءة؟
  - ما هي الفائدة المحتملة لتغيير أرقام الرقائق؟ **معايير النجاح**:
- تحديد حالتين على الأقل لاستخدام RFID في المتجر.
- وصف دقيق لنوع الرقاقة والفائدة.
- فقرة موجزة وواضحة مع صورة (إن وجدت). **تحدي إضافي**:
- تواصل مع موظف في المتجر (إذا أمكن) للسؤال عن نظام RFID الخاص بهم.
- ابحث عن مقال عبر الإنترنت يناقش استخدام RFID في متجر مشابه، وأضف رابطًا إلى ملاحظاتك.

مثال للإجابة:

- **الحالة 1**:
  - الوصف: ملصق RFID على بنطال في متجر H&M.
  - النوع: UHF (لنطاق القراءة الطويل في تتبع المخزون).
  - الفائدة: تغيير الرقم لتتبع دفعة جديدة أو تصحيح خطأ.
- **الحالة 2**:
  - الوصف: بوابة RFID عند مدخل المتجر لمنع السرقة.
  - النوع: UHF (للكشف عن الملصقات غير المعطلة).
  - الفائدة: إعادة برمجة الملصقات لتعطيلها بعد الدفع.
- **الفقرة**: "في زيارتي لمتجر H&M، لاحظت ملصقات RFID على الملابس، وهي على الأرجح UHF لتتبع المخزون بعيد المدى. كما رأيت بوابة RFID عند المدخل تكتشف الملصقات غير المعطلة لمنع السرقة. يعزز هذا النظام الكفاءة من خلال تسريع فحص المخزون وتقليل الأخطاء. تغيير أرقام الرقائق يساعد في تحديث بيانات المنتجات أو تصحيح الأخطاء، مما يضمن دقة التتبع."

1.11 النسخة الرقمية التفاعلية

موقع ويب تفاعلي (rfid-guide.x.ai):

- **التصميم**:
  - واجهة بسيطة بألوان (أزرق وأخضر) تتضمن قائمة فصول.
  - صفحة الفصل الأول تحتوي على:
    - نص الفصل مع صور مدمجة (مخطط تدفق، هيكلية MIFARE، دراسة حالة Zara).
    - فيديو "كيف تعمل RFID؟" (مدمج عبر YouTube).
    - رسم متحرك (30 ثانية) يُظهر تدفق البيانات.
    - أداة محاكاة: محاكي RFID يتيح للقارئ إدخال UID وهمي (مثل "A1B2C3D4") ورؤية كيف يعالج القارئ البيانات.
    - اختبار تفاعلي: 5 أسئلة (مثل "ما نوع الرقاقة في بطاقات المترو؟") مع تعليقات فورية.
- **الميزات**:
  - قسم "ملاحظاتي" لتسجيل إجابات التمرين (مثل ملاحظات زيارة المتجر).
  - منتدى للأسئلة والمناقشات.
  - روابط لتحميل تطبيقات (RFID TagInfo، NFC Tools).
- **الوصول**:
  - متاح عبر المتصفح على الهاتف/الكمبيوتر.
  - رمز QR في الكتاب المطبوع ينقل إلى الموقع.
- **مثال لأداة المحاكاة**:
  - واجهة تُظهر رقاقة وقارئ افتراضيين.
  - المستخدم يُدخل UID (مثل "12345678") ويختار "Read".
  - النتيجة: "UID: 12345678، النوع: MIFARE Classic، القطاعات: 16".

1.12 ملخص الفصل

- RFID هي تقنية تعتمد على موجات الراديو لنقل البيانات.
- تتكون من رقائق، قارئات، وبرمجيات، مع أنواع (LF، HF، UHF).
- هيكلية رقائق مثل MIFARE Classic تتيح الكتابة في قطاعات معينة.

- تاريخ RFID يمتد من الحرب العالمية إلى المدن الذكية.
- دراسة حالة Zara تُظهر كفاءة RFID في المخزون.
- التمرين العملي يربط المفاهيم بالواقع.

1.13 أسئلة مراجعة

- ما الفرق بين الرقائق النشطة والسلبية؟
- كيف تُستخدم رقائق UHF في Zara؟
- ما الذي يخزن في القطاع 0، الكتلة 0 في MIFARE Classic؟
- اذكر حدثًا رئيسيًا في تاريخ RFID من السبعينيات.

1.14 موارد إضافية

- فيديو: "كيف تعمل RFID؟" (youtube.com/rfid-how-it-works (#)).
- موقع: RFID Journal (rfidjournal.com).
- موقع الكتاب: rfid-guide.x.ai.
- تطبيقات: NFC Tools، RFID TagInfo.

1.3 مكونات نظام RFID

- **الرقاقة (Tag)**: تخزن بيانات (UID أو بيانات مخصصة)، نشطة أو سلبية.
- **القارئ (Reader)**: يرسل موجات راديو لقراءة/كتابة البيانات.
- **البرمجيات**: تعالج البيانات.

مخطط تدفق RFID:

[رقاقة RFID] ---> موجات راديو ---> [قارئ RFID] ---> USB/شبكة ---> [برمجيات/قاعدة بيانات]

- صورة ملونة تُظهر الرقاقة، القارئ، والبرمجيات.

1.4 أنواع رقائق RFID

- **LF (125-134 كيلوهرتز)**: نطاق قصير، للحيوانات وبطاقات الدخول.
- **HF (13.56 ميجاهرتز)**: نطاق متوسط، لبطاقات NFC والنقل.
- **UHF (860-960 ميجاهرتز)**: نطاق طويل، للمخزون واللوجستيات.

مخطط هيكلية MIFARE Classic:

- 16 قطاعًا، كل قطاع 4 كتل.

- القطاع 0، الكتلة 0: UID (غالبًا غير قابل للتعديل).
- الكتل الأخرى: بيانات قابلة للكتابة.
- رسم ملون يُظهر القطاعات مع تلوين (أحمر: UID، أخضر: بيانات، أزرق: مفاتيح).

1.5 الفرق بين الرقائق القابلة للكتابة والقراءة فقط

- **القراءة فقط:** بيانات ثابتة (مثل رقائق الحيوانات).
- **القراءة/الكتابة:** تتيح تعديل البيانات (مثل MIFARE).

1.6 مقارنة RFID مع الباركود *(قسم جديد)*

تقنية RFID والباركود تُستخدمان لتتبع الأغراض وإدارة البيانات، لكنهما يختلفان في الآلية، الأداء، والتطبيقات. فيما يلي مقارنة شاملة:

1. الآلية:

- **RFID:**
  - تعتمد على موجات الراديو لنقل البيانات.
  - الرقاقة ترسل البيانات (مثل UID) إلى القارئ عبر هوائي.
  - لا تتطلب رؤية مباشرة (يمكن قراءة الرقاقة داخل الصندوق أو الملابس).
- **الباركود:**
  - يعتمد على مسح بصري لرمز مطبوع (1D مثل UPC أو 2D مثل QR).
  - يتطلب رؤية مباشرة ومحاذاة الماسح مع الرمز.
  - مثال: ماسح الباركود في السوبرماركت يقرأ خطوط الرمز.

2. سعة التخزين:

- **RFID:**
  - تختزن بيانات أكبر (من بضعة بايتات إلى كيلوبايتات حسب الرقاقة).
  - يمكن تخزين UID، بيانات مخصصة، أو حتى سجلات (مثل تاريخ الإنتاج).
  - مثال: رقاقة MIFARE Classic 1K تخزن 1 كيلوبايت.
- **الباركود:**
  - سعة محدودة (عادةً بضع عشرات من الأحرف).
  - يخزن رقمًا تعريفيًا أو رابط URL (في QR).
  - مثال: باركود UPC يخزن 12 رقمًا.

3. سرعة القراءة:

- **RFID:**
  - قراءة فورية ومتعددة (يمكن قراءة مئات الرقائق في ثوانٍ).
  - مثال: قارئ UHF يفحص مخزون متجر بأكمله دفعة واحدة.
- **الباركود:**
  - قراءة بطيئة نسبيًا (يجب مسح كل رمز على حدة).
  - مثال: موظف الكاشير يمسح كل منتج يدويًا.

4. النطاق:

- **RFID:**
  - نطاق يتراوح من سنتيمترات (HF) إلى 15 مترًا (UHF).
  - مثال: تتبع شاحنة بضائع باستخدام UHF.
- **الباركود:**
  - نطاق قصير جدًا (بضعة سنتيمترات بين الماسح والرمز).
  - مثال: يجب وضع المنتج أمام الماسح مباشرة.

5. المتانة:

- **RFID:**
  - الرقائق مقاومة للعوامل البيئية (الماء، الغبار) إذا كانت مغلفة.
  - يمكن إعادة استخدامها (في الرقائق القابلة للكتابة).
- **الباركود:**
  - الرموز المطبوعة عرضة للتلف (تمزق، بهتان).
  - غير قابلة لإعادة البرمجة.

6. التكلفة:

- **RFID:**
  - تكلفة أعلى (رقاقة: 0.1-1 دولار، قارئ: 50-1000 دولار).
  - مثال: نظام RFID لمتجر يكلف آلاف الدولارات.
- **الباركود:**
  - تكلفة منخفضة (طباعة الرمز: أقل من سنت، ماسح: 20-100 دولار).
  - مثال: نظام الباركود شائع في المتاجر الصغيرة.

7. الأمان:

- **RFID:**
  - تدعم التشفير (مثل مفاتيح MIFARE)، مما يقلل من التزوير.
  - قابلة للكتابة، لكن قد تكون عرضة للهجمات إذا لم تُحمَ.
- **الباركود:**
  - لا يدعم التشفير، سهل التزوير (يمكن نسخ الرمز).
  - بيانات ثابتة، مما يقلل من المخاطر ولكنه يحد من المرونة.

8. التطبيقات:

- **RFID:**
  - إدارة المخزون، التحكم بالوصول، النقل العام، تتبع الحيوانات.
  - مثال: ملصقات RFID في Zara لتتبع الملابس.
- **الباركود:**
  - البيع بالتجزئة، تتبع الطرود، تذاكر الفعاليات.
  - مثال: رمز UPC على علبة الحليب.

جدول مقارنة (يُضاف في الكتاب):

الميزة	RFID	الباركود
الآلية	رؤيةبدون راديو، موجات	مباشرةرؤية بصري، مسح
سعة التخزين	(بايتات-كيلوبايتات)كبيرة	الأحرف)(عشرات محدودة
سرعة القراءة	متعددةفورية،	فرديةبطيئة،
النطاق	مترًا15 حتى	سنتيمتراتبضعة
المتانة	الاستخداملإعادة قابلة عالية،	للتلفعرضة منخفضة،
التكلفة	مرتفعة	منخفضة
الأمان	معقدلكنه تشفير،	التزويرسهل تشفير، بدون
التطبيقات	نقلدخول، مخزون،	تذاكرتجزئة، بيع

رسم توضيحي (يُضاف في الكتاب):

- صورة مقارنة تُظهر:
  - RFID: قارئ يفحص صندوق ملابس دفعة واحدة (UHF).
  - باركود: ماسح يقرأ رمزًا على علبة واحدة.
- تعليقات: "RFID: قراءة متعددة بدون رؤية"، "باركود: قراءة فردية برؤية".

أسئلة للتفكير:

- لماذا تُفضل المتاجر الكبيرة RFID على الباركود؟
- في أي سيناريو قد يكون الباركود أفضل من RFID؟

1.7 استخدامات RFID في الحياة اليومية

- التحكم بالوصول: بطاقات المكاتب.
- إدارة المخزون: ملصقات في المتاجر.
- النقل العام: بطاقات NFC.
- تتبع الحيوانات: رقائق مزروعة.

1.8 دراسة حالة: RFID في إدارة المخزون لدى Zara

- Zara تستخدم ملصقات UHF لتتبع الملابس.
- القارئات المحمولة تفحص المخزون بسرعة.
- تغيير الأرقام يساعد في تحديث البيانات.

مخطط: صورة تُظهر ملصق RFID وقارئ محمول.

1.9 لماذا تغيير أرقام RFID؟

- إعادة تخصيص الرقائق.
- إصلاح الأخطاء.
- التخصيص.
- التعلم.

1.10 كيف تعمل RFID؟ (فيديو توضيحي)

فيديو: "كيف تعمل RFID؟"

- مدة 3 دقائق، يوضح تدفق البيانات (رقاقة → قارئ → برمجيات).
- رسوم متحركة (30 ثانية) مدمجة.
- رابط: youtube.com/rfid-how-it-works (#).

1.11 تمرين عملي: قراءة UID فعليًا باستخدام هاتف ذكي أو قارئ RFID *(تمرين معدل)*

الهدف: تعلم كيفية قراءة المعرف الفريد (UID) لرقاقة RFID فعليًا، وربط المفاهيم بالتجربة التقنية. **الأدوات المطلوبة**:

- هاتف ذكي يدعم NFC (مثل معظم هواتف Android أو iPhone حديثة).
- تطبيق NFC Tools أو RFID TagInfo (مجاني، متاح على Google Play/App Store).
- رقاقة RFID (مثل بطاقة دخول، بطاقة مترو، أو ملصق NFC). إذا لم يكن لديك رقاقة، يمكنك استخدام بطاقة بنكية تدعم NFC.
- دفتر ملاحظات أو تطبيق تدوين.
- (اختياري) قارئ RFID USB (مثل ACR122U) مع كمبيوتر وبرنامج NFC Tools PC. **الخطوات**:
- **إعداد الأدوات**:
  - قم بتنزيل تطبيق NFC Tiles على هاتفك وتأكد من تفعيل NFC (في الإعدادات → اتصالات → NFC).
  - إذا كنت تستخدم قارئ USB، قم بتوصيله بالكمبيوتر وتثبيت التعريفات (رابط تعليمات في ملحق الكتاب).
- **تحديد رقاقة RFID**:
  - ابحث عن رقاقة في محيطك (مثل بطاقة دخول مكتب، بطاقة مترو، أو ملصق على منتج).
  - إذا لم تجد رقاقة، استخدم بطاقة بنكية تدعم NFC (تحتوي على رمز NFC).
- **قراءة UID**:
  - افتح تطبيق NFC Tools واختر خيار "Read" (قراءة).
  - ضع الرقاقة (أو البطاقة) بالقرب من الجزء الخلفي للهاتف (حيث مستشعر NFC).
  - انتظر حتى يظهر التطبيق بيانات الرقاقة (مثل UID، نوع الرقاقة، سعة التخزين).
  - إذا كنت تستخدم قارئ USB، ضع الرقاقة على القارئ وافتح برنامج NFC Tools PC لقراءة البيانات.
- **تسجيل النتائج**:

- دوّن المعلومات التالية:
  - **UID**: الرقم التعريفي (مثل "A1B2C3D4").
  - **نوع الرقاقة**: (مثل MIFARE Classic، NTAG، أو غير معروف إذا كانت بطاقة بنكية).
  - **التردد المحتمل**: LF، HF، أو UHF (استنادًا إلى الاستخدام، مثل HF لبطاقات الدخول).
  - **الاستخدام**: وصف سياق الرقاقة (مثل "بطاقة دخول للمكتب").
  - **ملاحظات إضافية**: هل الرقاقة محمية بكلمة مرور؟ هل يمكن كتابتها؟
- التقط لقطة شاشة للبيانات المعروضة في التطبيق.

- **تحليل النتائج**:
  - اكتب فقرة (100-150 كلمة) تجيب على:
    - ما نوع الرقاقة وكيف تُستخدم؟
    - هل يمكن تغيير UID أو البيانات بناءً على نوع الرقاقة؟ (استنادًا إلى الفصل: MIFARE قابلة للكتابة، بعض الرقائق للقراءة فقط).
    - كيف يمكن أن يفيد تغيير الرقم في هذا السياق؟ (مثل تخصيص بطاقة لشخص جديد).
- **إرسال النتائج** (اختياري):
  - إذا كنت تستخدم النسخة الرقمية (rfid-guide.x.ai)، قم برفع لقطة الشاشة وملاحظاتك إلى قسم "ملاحظاتي" في الموقع. **معايير النجاح**:
- قراءة UID بنجاح لـ رقاقة واحدة على الأقل.
- تسجيل بيانات دقيقة (UID، نوع، استخدام).
- فقرة تحليلية واضحة مع لقطة شاشة. **تحدي إضافي**:
- حاول قراءة رقاقتين مختلفتين (مثل بطاقة دخول وبطاقة بنكية) وقارن بياناتهما (هل هما من نفس النوع؟).
- ابحث عن نوع الرقاقة المحدد (مثل MIFARE Classic) عبر الإنترنت وأضف معلومات إضافية (مثل سعة التخزين أو مستوى التشفير).
- إذا كنت تمتلك قارئ USB، جرب قراءة الرقاقة باستخدام برنامج LibNFC (رابط في الملحقات) وسجل الفرق في الأداء مقارنة بالهاتف.

مثال للإجابة:

- **البيانات**:
  - UID: 04A1B2C3
  - نوع الرقاقة: MIFARE Classic 1K
  - التردد: HF (13.56 ميجاهرتز)
  - الاستخدام: بطاقة دخول لمبنى الجامعة
  - ملاحظات: الرقاقة محمية بمفتاح، لكن بعض القطاعات قابلة للكتابة
  - لقطة شاشة: [صورة تُظهر واجهة NFC Tools مع UID]
- **الفقرة**: "قرأت بطاقة دخول الجامعة باستخدام NFC Tools على هاتفي. الرقاقة من نوع MIFARE Classic 1K، تعمل على تردد HF، وتحمل UID: 04A1B2C3. تُستخدم لفتح أبواب المبنى، ويبدو أن بعض القطاعات قابلة للكتابة بناءً على بيانات التطبيق. تغيير الرقم قد يكون مفيدًا لتخصيص البطاقة لطالب جديد أو تحديث بيانات الوصول. الرقاقة محمية بمفتاح، مما يتطلب أذونات للتعديل. هذه التجربة ساعدتني على فهم كيفية عمل RFID عمليًا."

صورة توضيحية (يُضاف في الكتاب):

- لقطة شاشة نموذجية لواجهة NFC Tools تُظهر UID ونوع الرقاقة.
- صورة تُظهر هاتفًا يقرأ بطاقة دخول، مع تعليق: "ضع الرقاقة خلف الهاتف لقراءة UID."

1.12 ملخص الفصل

- RFID تعتمد على موجات الراديو لنقل البيانات، وتتكون من رقائق، قارئات، وبرمجيات.
- أنواع الرقائق: LF، HF، UHF، مع هيكلية مثل MIFARE Classic.
- RFID تتفوق على الباركود في السرعة، النطاق، والتخزين، لكنها أغلى.
- تاريخ RFID يمتد من الحرب العالمية إلى المدن الذكية.
- دراسة حالة Zara تُظهر كفاءة RFID في المخزون.
- التمرين العملي يتيح قراءة UID فعليًا لفهم التقنية تقنيًا.

1.13 أسئلة مراجعة

- ما الفرق بين رقائق LF وUHF من حيث النطاق والتطبيقات؟
- لماذا تُفضل RFID على الباركود في تتبع المخزون؟
- ما الذي يُخزن في الكتلة 0 من قطاع MIFARE Classic؟
- كيف ساعدت Zara رقائق RFID في تحسين عملياتها؟
- ما الذي تعلمته من قراءة UID في التمرين؟

1.14 موارد إضافية

- **فيديو**: "كيف تعمل RFID؟" (youtube.com/rfid-how-it-works (#)).
- **موقع**: rfid-guide.x.ai (لرفع نتائج التمرين ومشاهدة المحاكاة).
- **تطبيقات**: NFC Tools، RFID TagInfo.
- **برامج**: LibNFC لقارئات USB (رابط في الملحقات).

1.2 تاريخ RFID: رحلة التطور

- **1940s**: نظام IFF في الحرب العالمية.
- **1970s**: تتبع الماشية.
- **1990s**: رقائق HF (MIFARE) للنقل.
- **2025**: تكامل مع إنترنت الأشياء.

مخطط زمني: رسم بصري يُظهر المراحل (طائرة، بقرة، هاتف ذكي).

1.3 مكونات نظام RFID

- **الرقاقة**: تخزن UID أو بيانات، نشطة/سلبية.
- **القارئ**: يقرأ/يكتب البيانات.
- **البرمجيات**: تعالج البيانات.

مخطط تدفق:

[رقاقة RFID] --- موجات راديو ---> [قارئ USB] ---> [RFID/شبكة] ---> [برمجيات]

1.4 أنواع رقائق RFID

- **LF (125-134 كيلوهرتز)**: للحيوانات، الدخول.
- **HF (13.56 ميجاهرتز)**: NFC، النقل.
- **UHF (860-960 ميجاهرتز)**: المخزون، اللوجستيات.

مخطط MIFARE Classic:

- 16 قطاعًا، 4 كتل لكل قطاع.
- القطاع 0، الكتلة 0: UID.
- رسم ملون (أحمر: UID، أخضر: بيانات، أزرق: مفاتيح).

1.5 الفرق بين الرقائق القابلة للكتابة والقراءة فقط

- **القراءة فقط**: بيانات ثابتة.
- **القراءة/الكتابة**: تتيح التعديل.

1.6 مقارنة RFID مع الباركود

RFID والباركود تُستخدمان لتتبع الأغراض، لكنهما يختلفان في الآلية والأداء. إليك مقارنة تفصيلية:

- **الآلية**:
  - RFID: موجات راديو، بدون رؤية.
  - باركود: مسح بصري، رؤية مباشرة.
- **سعة التخزين**:
  - RFID: بايتات إلى كيلوبايتات (مثل MIFARE 1K).
  - باركود: عشرات الأحرف (مثل UPC: 12 رقمًا).
- **سرعة القراءة**:
  - RFID: فورية، متعددة.
  - باركود: بطيئة، فردية.
- **النطاق**:
  - RFID: حتى 15 مترًا (UHF).
  - باركود: سنتيمترات.
- **المتانة**:
  - RFID: مقاومة، قابلة لإعادة الاستخدام.
  - باركود: عرضة للتلف.
- **التكلفة**:
  - RFID: مرتفعة (رقاقة: 0.1-1 دولار).
  - باركود: منخفضة (سنتات).
- **الأمان**:
  - RFID: تشفير (مثل MIFARE).
  - باركود: بدون تشفير.
- **التطبيقات**:
  - RFID: مخزون، دخول.
  - باركود: بيع تجزئة، تذاكر.

جدول مقارنة (يُضاف في الكتاب):

الميزة	RFID	الباركود
الآلية	رؤيةبدون راديو، موجات	مباشرةرؤية بصري، مسح
سعة التخزين	(بايتات-كيلوبايتات)كبيرة	الأحرف)(عشرات محدودة
سرعة القراءة	متعددةفورية،	فرديةبطيئة،
النطاق	مترًا15 حتى	سنتيمتراتبضعة
المتانة	الاستخداملإعادة قابلة عالية،	للتلفعرضة منخفضة،
التكلفة	مرتفعة	منخفضة
الأمان	معقدلكنه تشفير،	التزويرسهل تشفير، بدون
التطبيقات	نقلدخول، مخزون،	تذاكرتجزئة، بيع

مخطط مقارنة RFID/باركود (تفصيلي):

- **الوصف البصري** (للصورة في الكتاب):
  - الصورة مقسمة إلى قسمين:
    - **الجانب الأيسر (RFID)**: قارئ UHF يفحص صندوق ملابس (يحتوي على 10 رقائق). موجات راديو تُرسم كخطوط متموجة تنتقل إلى شاشة كمبيوتر تُظهر قائمة بـ 10 UID (مثل "A1B2C3D4"). تعليق: "قراءة متعددة بدون رؤية، نطاق حتى 15 مترًا."
    - **الجانب الأيمن (باركود)**: موظف يمسح رمز UPC على علبة حليب باستخدام ماسح ليزر. شاشة الكاشير تُظهر رقمًا (مثل "012345678905"). تعليق: "قراءة فردية برؤية مباشرة، نطاق سنتيمترات."
  - في المنتصف: جدول مقارنة (كما أعلاه) مكتوب بخط صغير.
  - الألوان: أزرق لـ RFID (للإيحاء بالتكنولوجيا المتقدمة)، أحمر للباركود (للإيحاء بالبساطة).
  - أيقونات: رقاقة RFID (دائرة بهوائي)، باركود (خطوط أو QR).
- **تصميم ASCII** (تمثيل نصي للمخطط):

```
+----------------------------------+-----------------------------+
|              RFID                |           باركود            |
|----------------------------------|-----------------------------|
| [صندوق ملابس]                   | [علبة حليب]                 |
|    | 10 رقائق RFID               |    | رمز UPC                  |
|    v                             |    v                         |
| [قارئ UHF] ---- شعاع ---- [ماسح ليزر] | <---- موجات راديو ----> |
```

- **شرح ASCII**:
  - الجانب الأيسر يُظهر صندوقًا يحتوي على رقائق RFID تُقرأ دفعة واحدة.
  - الجانب الأيمن يُظهر علبة حليب مع رمز باركود يُمسح يدويًا.
  - الجدول في الأسفل يُلخص النطاق، التخزين، والأمان.
  - الموجات الراديو تُمثل بـ "---->"، والشعاع البصري كذلك.
- **الدمج في الكتاب**:
  - الصورة الملونة ستُضاف تحت عنوان "مخطط 1.2: مقارنة RFID وباركود".
  - تعليق: "يوضح هذا المخطط كيف تتفوق RFID في القراءة المتعددة والنطاق، بينما يبقى الباركود أبسط وأرخص."

أسئلة للتفكير:

- لماذا تُفضل RFID في تتبع المخزون مقارنة بالباركود؟
- متى يكون الباركود خيارًا أفضل (مثل متجر صغير)؟

1.7 استخدامات RFID في الحياة اليومية

- التحكم بالوصول.
- إدارة المخزون.
- النقل العام.
- تتبع الحيوانات.

1.8 دراسة حالة: RFID في Zara

- ملصقات UHF لتتبع الملابس.
- قارئات محمولة لفحص المخزون.
- تغيير الأرقام لتحديث البيانات.

1.9 لماذا تغيير أرقام RFID؟

- إعادة تخصيص.
- إصلاح الأخطاء.
- التخصيص.

1.10 كيف تعمل RFID؟ (فيديو توضيحي)

فيديو 1: "كيف تعمل RFID؟"

- مدة 3 دقائق، يوضح تدفق البيانات.

- رسوم متحركة (30 ثانية).
- رابط: youtube.com/rfid-how-it-works (#).

فيديو 2: "RFID مقابل الباركود" *(فيديو إضافي)*

- **المدة**: 4 دقائق.
- **المحتوى**:
  - **المقدمة (30 ثانية)**: شرح مختصر لـ RFID والباركود كتقنيتين لتتبع الأغراض. لقطات: قارئ RFID يفحص صندوق، ماسح باركود يقرأ علبة.
  - **المقارنة (2.5 دقيقة)**:
    - **الآلية**: رسوم متحركة تُظهر موجات راديو لـ RFID (رقاقة تُضيء وترسل UID) مقابل شعاع ليزر للباركود (رمز يُمسح).
    - **الأداء**: مقطع يُظهر قارئ UHF يقرأ 10 رقائق دفعة واحدة في متجر، مقابل موظف يمسح 10 منتجات يدويًا.
    - **التطبيقات**: لقطات واقعية: RFID في بوابة متجر Zara، باركود في سوبرماركت صغير.
    - **التكلفة والأمان**: رسم بياني يقارن التكلفة (عالية لـ RFID، منخفضة للباركود) والأمان (تشفير لـ RFID، لا يوجد للباركود).
  - **الخاتمة (1 دقيقة)**: تلخيص المزايا (RFID: سرعة ومرونة، باركود: بساطة وتكلفة). دعوة للتفكير: "أي تقنية تُفضل لمتجرك؟".
- **الإنتاج**:
  - أدوات: Adobe Premiere لتحرير الفيديو، After Effects للرسوم المتحركة.
  - تعليق صوتي عربي واضح، ترجمات إنجليزية.
  - لقطات واقعية من متاجر (بإذن) أو لقطات تخزين (Stock Footage).
  - استضافة على يوتيوب: youtube.com/rfid-vs-barcode (#).
- **الدمج في الكتاب**:
  - رمز QR تحت عنوان "مخطط 1.2" ينقل إلى الفيديو.
  - تعليق: "شاهد فيديو ’RFID مقابل الباركود‘ لفهم الاختلافات بصريًا."

1.11 تمرين عملي: قراءة UID وتجربة كتابة بيانات بسيطة *(تمرين معدل)*

الهدف: تعلم قراءة المعرف الفريد (UID) لرقاقة RFID وتجربة كتابة بيانات بسيطة (إذا كانت الرقاقة تدعم الكتابة) لفهم RFID عمليًا. **الأدوات المطلوبة**:

- هاتف ذكي يدعم NFC (Android أو iPhone حديث).
- تطبيق NFC Tools (مجاني على Google Play/App Store).
- رقاقة RFID (مثل بطاقة دخول، بطاقة مترو، ملصق NFC). للكتابة، يجب أن تكون الرقاقة قابلة للكتابة (مثل MIFARE Classic أو NTAG213).
- (اختياري) قارئ USB (مثل ACR122U) مع برنامج NFC Tools PC.
- دفتر ملاحظات أو تطبيق تدوين. **الخطوات**:
- **إعداد الأدوات**:
  - نزّل NFC Tools وفعّل NFC في إعدادات الهاتف (اتصالات → NFC).
  - إذا كنت تستخدم قارئ USB، وصّله بالكمبيوتر وثبّت التعريفات (رابط في الملحقات).
- **تحديد رقاقة RFID**:

- ابحث عن رقاقة (بطاقة دخول، بطاقة مترو، ملصق NFC). إذا لم يكن لديك، جرب بطاقة بنكية تدعم NFC (للقراءة فقط).
- للكتابة، تأكد من أن الرقاقة قابلة للكتابة (مثل ملصق NTAG213 أو MIFARE Classic غير محمية).

- **قراءة UID**:
  - افتح NFC Tools واختر "Read".
  - ضع الرقاقة خلف الهاتف (حيث مستشعر NFC) أو على القارئ.
  - سجّل البيانات: UID (مثل "04A1B2C3")، نوع الرقاقة (مثل MIFARE)، التردد (HF؟)، الاستخدام (مثل "بطاقة دخول").
  - التقط لقطة شاشة لواجهة التطبيق.
- **تجربة كتابة بيانات بسيطة** (إذا كانت الرقاقة تدعم):
  - في NFC Tools، تحقق مما إذا كانت الرقاقة قابلة للكتابة (تظهر خيارات "Write" إذا كانت كذلك).
  - اختر "Write" → "Add a Record" → "Text Record".
  - أدخل نصًا بسيطًا (مثل "Test123" أو اسمك).
  - ضع الرقاقة خلف الهاتف واضغط "Write".
  - اقرأ الرقاقة مرة أخرى للتحقق مما إذا كُتب النص (في قسم "Data" بالتطبيق).
  - إذا فشلت الكتابة (مثل رقاقة محمية أو للقراءة فقط)، دوّن السبب (مثل "الرقاقة محمية بمفتاح").
  - **ملاحظة أمان**: لا تكتب على بطاقات مهمة (مثل بطاقة دخول عمل) لأن ذلك قد يؤدي إلى تعطيلها. استخدم ملصقات NFC رخيصة للتجربة.
- **تسجيل النتائج**:
  - دوّن:
    - **UID**: (مثل "04A1B2C3").
    - **نوع الرقاقة**: (مثل MIFARE Classic).
    - **التردد**: (HF، استنادًا إلى الاستخدام).
    - **الاستخدام**: (مثل "بطاقة مترو").
    - **نتيجة الكتابة**: (مثل "كتبت ‘Test123’ بنجاح" أو "فشلت بسبب الحما...

مخطط مقارنة RFID/باركود (تفصيلي جدًا):

- **الوصف البصري (للصورة في الكتاب):**
  - الصورة مقسمة إلى ثلاثة أجزاء رئيسية:
    - **الجزء العلوي: العملية:**
      - **RFID**: مشهد يُظهر مستودعًا مع قارئ UHF محمول يفحص صندوقًا يحتوي على 20 منتجًا (كل منتج به رقاقة RFID). موجات راديو تُرسم كدوائر متحدة المركز تنبعث من القارئ. شاشة الكمبيوتر تُظهر قائمة بـ 20 UID (مثل "A1B2C3D4"، "B2C3D4E5"") مع بيانات إضافية (مثل "قميص أزرق، مقاس M"). تعليق: "قراءة متعددة بدون رؤية، نطاق حتى 15 مترًا، تخزين كيلوبايتات."
      - **باركود**: مشهد يُظهر موظف سوبرماركت يمسح رمز UPC على علبة حليب باستخدام ماسح ليزر. شعاع أحمر يربط الماسح بالرمز. شاشة الكاشير تُظهر رقمًا (مثل "012345678905") وبيانات محدودة (مثل "حليب 1 لتر"). تعليق: "قراءة فردية برؤية مباشرة، نطاق سنتيمترات، تخزين أحرف."

- **الجزء الوسطي: الجدول**:
  - جدول المقارنة (كما أعلاه) مكتوب بخط واضح، مع تظليل باللون الأزرق لـ RFID والأحمر للباركود.
  - أيقونات بجانب كل ميزة: موجات راديو للآلية RFID، عين للباركود؛ ذاكرة للتخزين RFID، ورقة للباركود.
- **الجزء السفلي: التطبيقات**:
  - **RFID**: صور مصغرة تُظهر ملصق RFID على سترة في Zara، بطاقة دخول مكتب، بطاقة مترو NFC.
  - **باركود**: صور مصغرة تُظهر رمز UPC على علبة، رمز QR على تذكرة، رمز على طرد بريدي.
- **الألوان**: أزرق/أخضر لـ RFID (تكنولوجيا متقدمة)، أحمر/أسود للباركود (بساطة).
- **التصميم**: يُستخدم برنامج Adobe Illustrator لإنشاء الصورة، مع خطوط نظيفة وتعليقات موجزة.
- **التعليق في الكتاب**: "مخطط 1.2: يوضح هذا المخطط كيف تتفوق RFID في القراءة المتعددة، النطاق الطويل، والتخزين الكبير، بينما يبقى الباركود أرخص وأبسط للمتاجر الصغيرة."

- **تصميم ASCII متقدم** (تمثيل نصي للمخطط):
- **شرح ASCII**:

```
+-------------------------------------------------------+
|                    مقارنة RFID وباركود              |
+-------------------------------+-----------------------+
|             RFID              |       باركود         |
+-------------------------------+-----------------------+
| [مستودع]                    | [سوبرماركت]        |
|  [صندوق]                     |   [علبة حليب]      |
|   | 20 رقاقة RFID          |    | رمز UPC           |
|   |  [رقاقة] [رقاقة] ...   |    | [||||||]          |
|   v                           |   v                   |
| [قارئ UHF]                   | [ماسح ليزر]        |
|   |~~~~ شعاع ---|    |    ~~~~ موجات راديو ---     |
|   v                           |   v                   |
| [كمبيوتر]                    | [شاشة كاشير]       |
|  UID: A1B2C3D4 (قميص M)    |  012345678905 :رقم  |
|  UID: B2C3D4E5 (قميص L)    |  (حليب 1 لتر)       |
|  ... (20 رقاقة)              |                       |
| * قراءة فردية * |             قراءة متعددة        |
| * نطاق: سنتيمترات * |           نطاق: حتى 15م   |
| * تخزين: أحرف * |         تخزين: كيلوبايتات      |
+-------------------------------+-----------------------+
| تطبيقات |                       :تطبيقات:         |
| - ملصق Zara                  | - رمز UPC           |
| - رمز - |                  بطاقة دخول QR          |
| - طرد بريدي - |                 بطاقة مترو       |
+-------------------------------+-----------------------+
| جدول مقارنة:                                        |
| ميزة     | RFID          | باركود                  |
|---------|---------------|------------------------|
| مسح بصري | موجات راديو |     آلية               |
| محدود |         كبير |    تخزين                 |
| بطيئة |        فورية |    سرعة                  |
| لا يوجد |        تشفير |     أمان               |
+-------------------------------------------------------+
```

- **الجزء العلوي**: يُظهر RFID في مستودع (صندوق به 20 رقاقة، قارئ UHF يقرأ الجميع دفعة واحدة) مقابل باركود في سوبرماركت (علبة حليب، ماسح يقرأ رمزًا واحدًا).
- **موجات راديو**: تُمثل بـ "~~~" لإيحاء الترددات.
- **شعاع الليزر**: تُمثل بـ "---" لإيحاء المسح البصري.
- **الشاشة**: RFID تُظهر قائمة UID مع بيانات (مثل المقاس)، باركود تُظهر رقمًا وبيانات محدودة.
- **الجزء الوسطي**: قائمة تطبيقات بأيقونات نصية (مثل "[رقاقة]" لـ RFID).
- **الجزء السفلي**: جدول مقارنة موجز.

- **الدمج في الكتاب**:
  - الصورة الملونة (مصممة بـ Adobe Illustrator) تُضاف تحت عنوان "مخطط 1.2".
  - تعليق: "يوضح المخطط العمليات والتطبيقات لكل تقنية، مع جدول يُبرز الفروقات الرئيسية."

أسئلة للتفكير:

- كيف يساعد النطاق الطويل لـ RFID في إدارة المستودعات؟
- لماذا يُفضل الباركود في متاجر البقالة الصغيرة؟

1.7 استخدامات RFID في الحياة اليومية

- التحكم بالوصول.
- إدارة المخزون.
- النقل العام.
- تتبع الحيوانات.

1.8 دراسة حالة: RFID في Zara

- ملصقات UHF لتتبع الملابس.
- قارئات محمولة لفحص المخزون.
- تغيير الأرقام لتحديث البيانات.

1.9 لماذا تغيير أرقام RFID؟

- إعادة تخصيص.
- إصلاح الأخطاء.
- التخصيص.

1.10 كيف تعمل RFID؟ (فيديو توضيحي)

فيديو 1: "كيف تعمل RFID؟"

- مدة 3 دقائق، يوضح تدفق البيانات.
- رابط: youtube.com/rfid-how-it-works (#).

فيديو 2: "RFID مقابل الباركود" *(فيديو إضافي)*

- **المدة**: 4 دقائق.
- **المحتوى**:
  - **المقدمة (30 ثانية)**: مقدمة عن RFID والباركود كتقنيتين لتتبع الأغراض. لقطات: قارئ RFID يفحص صندوق في مستودع، ماسح باركود يقرأ علبة في متجر.
  - **المقارنة (2.5 دقيقة)**:
    - **الآلية**: رسوم متحركة تُظهر موجات راديو تنبعث من قارئ RFID لتنشيط رقاقة (تُضيء وترسل UID)، مقابل شعاع ليزر يمسح رمز باركود (خطوط تُضيء على الرمز).
    - **الأداء**: مقطع يُظهر قارئ UHF يقرأ 20 رقاقة في ثوانٍ (شاشة تُظهر قائمة UID)، مقابل موظف يمسح 20 منتجًا يدويًا (يستغرق دقائق).
    - **التطبيقات**: لقطات: RFID في Zara (ملصق على سترة)، بطاقة مترو NFC، مقابل باركود على علبة حليب، رمز QR على تذكرة.
    - **التكلفة والأمان**: رسم بياني يقارن التكلفة (عمود مرتفع لـ RFID، منخفض للباركود) والأمان (رمز قفل لـ RFID، بدون قفل للباركود).
  - **الخاتمة (1 دقيقة)**: تلخيص: "RFID مثالية للتتبع السريع والمرن، بينما الباركود أرخص وأبسط." دعوة: "فكر في متجرك، أي تقنية تختار؟".
- **نص صوتي جزئي (للمقدمة والآلية)**:
  - **المقدمة**: "مرحبًا! اليوم، سنستكشف تقنيتين أساسيتين لتتبع الأغراض: RFID والباركود. RFID تستخدم موجات الراديو لقراءة البيانات عن بُعد، بينما الباركود يعتمد على المسح البصري. دعونا نقارن بينهما!"
  - **الآلية**: "في RFID، يرسل القارئ موجات راديو لتنشيط الرقاقة، التي ترسل معرفها الفريد، حتى لو كانت داخل صندوق. أما الباركود، فيتطلب مسحًا بصريًا مباشرًا باستخدام ليزر أو كاميرا، مما يعني أنك بحاجة إلى رؤية الرمز بوضوح."
- **الإنتاج**:
  - أدوات: Adobe Premiere (تحرير)، After Effects (رسوم متحركة).
  - تعليق صوتي عربي، ترجمات إنجليزية.
  - لقطات واقعية (بإذن) أو لقطات تخزين.
  - استضافة: youtube.com/rfid-vs-barcode (#).
- **الدمج**:
  - رمز QR تحت "مخطط 1.2".
  - تعليق: "شاهد فيديو 'RFID مقابل الباركود' لفهم الفروقات بصريًا."

1.11 تمرين عملي: قراءة UID وكتابة بيانات بسيطة مع تحليل (*تمرين معدل*)

الهدف: تعلم قراءة المعرف الفريد (UID) لرقاقة RFID، تجربة كتابة بيانات بسيطة (إذا كانت الرقاقة تدعم)، وتحليل البيانات المكتوبة باستخدام تطبيق آخر لفهم RFID عمليًا. **الأدوات المطلوبة**:

- هاتف ذكي يدعم NFC (Android أو iPhone حديث).
- تطبيقات: NFC Tools وRFID TagInfo (مجانية على Google Play/App Store).
- رقاقة RFID قابلة للكتابة (مثل ملصق NTAG213 أو MIFARE Classic غير محمية). للقراءة فقط، استخدم بطاقة دخول أو بطاقة بنكية NFC.
- (اختياري) قارئ USB (مثل ACR122U) مع NFC Tools PC.
- دفتر ملاحظات أو تطبيق تدوين. **الخطوات**:
- **إعداد الأدوات**:
  - نزّل NFC Tools وRFID TagInfo، فعّل NFC (إعدادات ← اتصالات ← NFC).

- إذا كنت تستخدم قارئ USB، وصّله وثبّت التعريفات (رابط في الملحقات).
- **تحديد رقاقة RFID**:
  - اختر رقاقة (بطاقة دخول، ملصق NFC، بطاقة مترو). للكتابة، استخدم ملصق NTAG213 أو رقاقة غير محمية.
  - **تحذير أمان**: لا تكتب على بطاقات مهمة (مثل بطاقة عمل) لأن ذلك قد يعطلها.
- **قراءة UID**:
  - افتح NFC Tools، اختر "Read".
  - ضع الرقاقة خلف الهاتف أو على القارئ.
  - سجّل: UID (مثل "04A1B2C3")، نوع الرقاقة (مثل NTAG213)، التردد (HF؟)، الاستخدام (مثل "ملصق NFC").
  - التقط لقطة شاشة.
- **كتابة بيانات بسيطة** (إذا كانت الرقاقة تدعم):
  - في NFC Tools، تحقق من خيار "Write" (يظهر إذا كانت الرقاقة قابلة للكتابة).
  - اختر "Write" → "Add a Record" → "Text Record".
  - أدخل نصًا (مثل "MyRFIDTest2025").
  - ضع الرقاقة خلف الهاتف واضغط "Write".
  - إذا فشلت الكتابة (مثل رقاقة محمية)، دوّن السبب (مثل "مفتاح تشفير مطلوب").
- **تحليل البيانات المكتوبة**:
  - افتح RFID TagInfo وأعد قراءة الرقاقة.
  - تحقق مما إذا كُتب النص (يظهر في قسم "Data" أو "NDEF Records").
  - قارن البيانات بين NFC Tools وRFID TagInfo (هل النص متطابق؟ هل هناك بيانات إضافية؟).
  - سجّل: النص المكتوب، تنسيق البيانات (مثل NDEF)، أي اختلافات.
- **تسجيل النتائج**:
  - دوّن:
    - **UID**: (مثل "04A1B2C3").
    - **نوع الرقاقة**: (مثل NTAG213).
    - **التردد**: (HF).
    - **الاستخدام**: (مثل "ملصق NFC للتجربة").
    - **نتيجة الكتابة**: (مثل "كتبت 'MyRFIDTest2025' بنجاح" أو "فشلت بسبب الحماية").
    - **تحليل البيانات**: (مثل "النص ظهر في RFID TagInfo كنص NDEF، بدون اختلافات").
    - **لقطات شاشة**: واجهة NFC Tools (قراءة/كتابة)، واجهة RFID TagInfo (تحليل).
- **تحليل النتائج**:
  - اكتب فقرة (150-200 كلمة):
    - وصف الرقاقة واستخدامها.
    - هل يمكن تغيير البيانات؟ لماذا؟
    - كيف يفيد تغيير الرقم/البيانات؟
    - ما تعلمته من الكتابة والتحليل (مثل تنسيق NDEF أو قيود التشفير).
- **إرسال النتائج** (اختياري):
  - ارفع لقطات الشاشة وملاحظاتك إلى rfid-guide.x.ai (قسم "ملاحظاتي"). **معايير النجاح**:
- قراءة UID بنجاح.
- محاولة كتابة بيانات (حتى لو فشلت) مع تسجيل السبب.
- تحليل البيانات باستخدام RFID TagInfo.

- فقرة تحليلية مع لقطتي شاشة. **تحدي إضافي**:
- جرب كتابة رابط URL (مثل "https://x.ai") بدلًا من نص، ثم افتح الرابط بقارئ NFC آخر (مثل هاتف مختلف).
- قارن قراءة/كتابة بين رقاقتين (مثل NTAG213 وMIFARE).
- إذا كنت تستخدم قارئ USB، جرب LibNFC لكتابة البيانات وسجل الفرق.

مثال للإجابة:

- **البيانات**:
  - UID: 04A1B2C3
  - نوع الرقاقة: NTAG213
  - التردد: HF
  - الاستخدام: ملصق NFC للتجربة
  - نتيجة الكتابة: كتبت "MyRFIDTest2025" بنجاح
  - تحليل: النص ظهر في RFID TagInfo كنص NDEF، بدون اختلافات
  - لقطات شاشة: [NFC Tools: UID وكتابة]، [RFID TagInfo: نص NDEF]
- **الفقرة**: "استخدمت NFC Tools لقراءة ملصق HF (NTAG213) مع UID: 04A1B2C3، وهو ملصق NFC اشتريته للتجربة. قرأت البيانات بنجاح، ثم كتبت نص 'MyRFIDTest2025' باستخدام خيار Text Record. أعدت القراءة بـ RFID TagInfo، وأظهر النص كنص NDEF دون أخطاء. الكتابة كانت ممكنة لأن NTAG213 غير محمية وتدعم الكتابة. تغيير البيانات مفيد لتخصيص الملصق، مثل إضافة بيانات مشروع. تعلمت أن تنسيق NDEF يجعل البيانات قابلة للقراءة عبر تطبيقات متعددة، وأن ال الحماية تحد من الكتابة في الرقائق الحساسة."

صورة توضيحية:

- لقطات شاشة لـ NFC Tools (قراءة/كتابة) وRFID TagInfo (تحليل).
- صورة لهاتف يقرأ ملصق NFC، مع تعليق: "ضع الرقاقة هنا للقراءة/الكتابة."

1.12 ملخص الفصل

- RFID تستخدم موجات الراديو، مع رقائق (LF، HF، UHF).
- تتفوق على الباركود في السرعة، النطاق، والتخزين، لكنها أغلى.
- هيكلية MIFARE Classic تتيح الكتابة في قطاعات.
- تاريخ RFID من 1940s إلى 2025.
- دراسة حالة Zara تُظهر كفاءة RFID.
- التمرين يتيح قراءة UID، كتابة بيانات، وتحليلها.

1.13 أسئلة مراجعة

- كيف يختلف نطاق RFID عن الباركود؟
- لماذا تُستخدم RFID في Zara؟
- ما الذي يُخزن في قطاع MIFARE Classic؟
- ماذا تعلمت من قراءة UID وكتابة البيانات؟

1.14 موارد إضافية

- **فيديوهات**:
  - "كيف تعمل RFID؟" (youtube.com/rfid-how-it-works (#)).
  - "RFID مقابل الباركود" (youtube.com/rfid-vs-barcode (#)).
- **موقع**: rfid-guide.x.ai.
- **تطبيقات**: NFC Tools، RFID TagInfo.
- **برامج**: LibNFC.

1.3 مكونات نظام RFID

- **الرقاقة**: تخزن UID أو بيانات، نشطة/سلبية.
- **القارئ**: يقرأ/يكتب البيانات.
- **البرمجيات**: تعالج البيانات.

مخطط تدفق:

[رقاقة RFID] <--- موجات راديو ---> [قارئ USB ---> [RFID/شبكة ---> [برمجيات]

1.4 أنواع رقائق RFID

- **LF (125-134 كيلوهرتز)**: للحيوانات، الدخول.
- **HF (13.56 ميجاهرتز)**: NFC، النقل.
- **UHF (860-960 ميجاهرتز)**: المخزون، اللوجستيات.

مخطط MIFARE Classic: 16 قطاعًا، UID في القطاع 0، رسم ملون (أحمر: UID، أخضر: بيانات، أزرق: مفاتيح).

1.5 الفرق بين الرقائق القابلة للكتابة والقراءة فقط

- **القراءة فقط**: بيانات ثابتة.
- **القراءة/الكتابة**: تتيح التعديل.

1.6 مقارنة RFID مع الباركود

- **الآلية**: RFID (موجات راديو)، باركود (مسح بصري).
- **سعة التخزين**: RFID (كيلوبايتات)، باركود (أحرف).
- **النطاق**: RFID (حتى 15 مترًا)، باركود (سنتيمترات).
- **التكلفة**: RFID (مرتفعة)، باركود (منخفضة).

مخطط 1.2: يُظهر RFID (قراءة متعددة في مستودع) مقابل باركود (قراءة فردية في سوبرماركت).

1.7 مقارنة RFID مع NFC *(قسم جديد)*

تقنية **الاتصال قريب المدى (NFC)** غالبًا تُعتبر جزءًا من RFID، لكنها تتميز بخصائص محددة تجعلها مناسبة لتطبيقات معينة. إليك مقارنة بين RFID وNFC:

- **1. التعريف**:
  - **RFID**: تقنية عامة لنقل البيانات عبر موجات الراديو، تشمل ترددات LF، HF، وUHF.

- **NFC**: نوع من RFID يعمل فقط على HF (13.56 ميجاهرتز)، مصمم للاتصال ثنائي الاتجاه في نطاق قصير جدًا.
- **2. التردد**:
  - **RFID**: LF (125-134 كيلوهرتز)، HF (13.56 ميجاهرتز)، UHF (860-960 ميجاهرتز).
  - **NFC**: HF فقط، يتبع معايير ISO/IEC 14443 و18092.
- **3. النطاق**:
  - **RFID**: من سنتيمترات (HF) إلى 15 مترًا (UHF).
  - **NFC**: حتى 10 سم (عادةً 4 سم)، لضمان الأمان.
- **4. الاتصال**:
  - **RFID**: أحادي الاتجاه (رقاقة إلى قارئ) أو محدود ثنائي (HF).
  - **NFC**: ثنائي الاتجاه، يدعم:
    - **قراءة/كتابة**: قراءة ملصق NFC (مثل رابط URL).
    - **Peer-to-Peer**: تبادل البيانات (مثل مشاركة صورة).
    - **محاكاة البطاقة**: الهاتف كبطاقة دفع.
- **5. التطبيقات**:
  - **RFID**: تتبع المخزون (UHF)، التحكم بالوصول (HF)، تتبع الحيوانات (LF).
  - **NFC**: الدفع بدون تلامس (Apple Pay)، مشاركة البيانات، ملصقات ذكية.
- **6. الأجهزة**:
  - **RFID**: قارئات مخصصة (مثل ACR122U لـ HF، قارئات UHF للمستودعات).
  - **NFC**: مدمجة في الهواتف الذكية، مما يجعلها متاحة.
- **7. الأمان**:
  - **RFID**: يعتمد على الرقاقة (مثل تشفير MIFARE)، لكن UHF قد يكون أقل أمانًا.
  - **NFC**: تشفير قوي (مثل في الدفع)، نطاق قصير يقلل من الاختراق.

جدول مقارنة (يُضاف في الكتاب):

الميزة	RFID	NFC
التردد	،LF ،HFUHF	HF 13.56)(ميجاهرتز
النطاق	مترًا15 حتى	سم10 حتى
الاتصال	محدودأحادي/ثنائي	أوضاع)(3 ثنائي
التطبيقات	حيواناتدخول، مخزون،	بياناتمشاركة ملصقات، دفع،
الأجهزة	مخصصةقارئات	HFقارئات ذكية، هواتف
الأمان	الرقاقةعلى يعتمد	قصيرنطاق قوي، تشفير

رسم توضيحي (يُضاف في الكتاب):

- صورة مقسمة:
  - **RFID**: قارئ UHF يفحص صندوق مخزون (نطاق طويل)، بطاقة دخول HF.
  - **NFC**: هاتف يقرأ ملصق NFC (رابط URL)، هاتف آخر يدفع عبر NFC.
- تعليق: "NFC هي RFID بتردد HF، مصممة للاتصال القريب والتطبيقات الاستهلاكية."

أسئلة للتفكير:

- لماذا يُستخدم NFC في الدفع وليس UHF RFID؟
- كيف يساعد النطاق القصير لـ NFC في الأمان؟

1.8 استخدامات RFID في الحياة اليومية

- التحكم بالوصول.
- إدارة المخزون.
- النقل العام.
- تتبع الحيوانات.

1.9 دراسة حالة: RFID في Zara

- ملصقات UHF لتتبع الملابس.
- قارئات محمولة لفحص المخزون.
- تغيير الأرقام لتحديث البيانات.

1.10 لماذا تغيير أرقام RFID؟

- إعادة تخصيص.
- إصلاح الأخطاء.
- التخصيص.

1.11 كيف تعمل RFID؟ (فيديو توضيحي)

- **فيديو 1**: "كيف تعمل RFID؟" (3 دقائق).
- **فيديو 2**: "RFID مقابل الباركود" (4 دقائق).
- **ملاحظة**: يمكن إضافة فيديو "RFID مقابل NFC" لاحقًا (غير مدرج حاليًا).

1.12 تمرين عملي: قراءة UID، كتابة بيانات، واختبار بجهاز آخر *(تمرين معدل)*

الهدف: تعلم قراءة المعرف الفريد (UID) لرقاقة RFID، كتابة بيانات بسيطة (إذا كانت تدعم)، واختبار البيانات المكتوبة باستخدام جهاز آخر (مثل قارئ USB) لفهم RFID عمليًا. **الأدوات المطلوبة**:

- هاتف ذكي يدعم NFC (Android أو iPhone حديث).
- تطبيقات: NFC Tools، RFID TagInfo (مجانية على Google Play/App Store).

- رقاقة RFID قابلة للكتابة (مثل ملصق NTAG213 أو MIFARE Classic غير محمية). للقراءة فقط، استخدم بطاقة دخول أو بطاقة بنكية NFC.
- قارئ USB (مثل ACR122U) مع كمبيوتر وبرنامج NFC Tools PC أو LibNFC.
- دفتر ملاحظات أو تطبيق تدوين. **الخطوات**:
- **إعداد الأدوات**:
  - نزّل NFC Tools وRFID TagInfo على الهاتف، فعّل NFC (إعدادات → اتصالات → NFC).
  - للقارئ USB، وصّله بالكمبيوتر، ثبّت التعريفات، ونزّل NFC Tools PC أو LibNFC (رابط في الملحقات).
- **تحديد رقاقة RFID**:
  - اختر رقاقة (ملصق NTAG213، بطاقة دخول، بطاقة مترو). للكتابة، تأكد من أنها قابلة للكتابة (NTAG213 أو MIFARE غير محمية).
  - **تحذير أمان**: لا تكتب على بطاقات حساسة (مثل بطاقة عمل) لتجنب تعطيلها.
- **قراءة UID**:
  - افتح NFC Tools على الهاتف، اختر "Read".
  - ضع الرقاقة خلف الهاتف (مستشعر NFC).
  - سجّل: UID (مثل "04A1B2C3")، نوع الرقاقة (مثل NTAG213)، التردد (HF)، الاستخدام (مثل "ملصق NFC").
  - التقط لقطة شاشة.
- **كتابة بيانات بسيطة**:
  - في NFC Tools، تحقق من خيار "Write" (يظهر إذا كانت الرقاقة قابلة للكتابة).
  - اختر "Write" → "Add a Record" → "Text Record".
  - أدخل نصًا (مثل "MyRFIDTest2025").
  - ضع الرقاقة خلف الهاتف واضغط "Write".
  - إذا فشلت الكتابة (مثل رقاقة محمية)، دوّن السبب (مثل "مطلوب مفتاح تشفير").
- **اختبار البيانات بجهاز آخر (قارئ USB)**:
  - وصّل قارئ USB (مثل ACR122U) بالكمبيوتر.
  - افتح NFC Tools PC، ضع الرقاقة على القارئ، واختر "Read".
  - تحقق مما إذا كُتب النص (مثل "MyRFIDTest2025") في قسم "Data" أو "NDEF Records".
  - قارن البيانات مع قراءة الهاتف (هل النص متطابق؟ هل هناك اختلافات في التنسيق؟).
  - (اختياري) استخدم LibNFC لقراءة البيانات بشكل أعمق (مثل عرض القطاعات في MIFARE).
  - سجّل: النص المقروء، التنسيق (مثل NDEF)، أي اختلافات، ملاحظات عن أداء القارئ USB مقارنة بالهاتف.
  - التقط لقطة شاشة لواجهة NFC Tools PC أو LibNFC.
- **تسجيل النتائج**:
  - دوّن:
    - **UID**: (مثل "04A1B2C3").
    - **نوع الرقاقة**: (مثل NTAG213).
    - **التردد**: (HF).
    - **الاستخدام**: (مثل "ملصق NFC للتجربة").
    - **نتيجة الكتابة**: (مثل "كتبت ‘MyRFIDTest2025’ بنجاح").
    - **اختبار الجهاز الآخر**: (مثل "النص ظهر في NFC Tools PC كنص NDEF، متطابق مع الهاتف").

- **لقطات شاشة**: واجهة NFC Tools (هاتف)، NFC Tools PC أو LibNFC (قارئ USB).
- **تحليل النتائج**:
  - اكتب فقرة (150-200 كلمة):
    - وصف الرقاقة واستخدامها.
    - هل يمكن تغيير البيانات؟ لماذا؟
    - كيف يفيد تغيير البيانات؟
    - ما تعلمته من الكتابة واختبار البيانات بجهاز آخر (مثل دقة القارئ USB أو تنسيق NDEF).
- **إرسال النتائج** (اختياري):
  - ارفع لقطات الشاشة وملاحظاتك إلى rfid-guide.x.ai (قسم "ملاحظاتي"). **معايير النجاح**:
- قراءة UID بنجاح على الهاتف.
- محاولة كتابة بيانات (حتى لو فشلت) مع تسجيل السبب.
- اختبار البيانات بقارئ USB (أو جهاز آخر) مع مقارنة النتائج.
- فقرة تحليلية مع لقطتي شاشة (هاتف وقارئ USB). **تحدي إضافي**:
- جرب كتابة رابط URL (مثل "https://x.ai") واختبره بقارئ USB أو هاتف آخر (هل يفتح الرابط؟).
- إذا استخدمت LibNFC، حاول قراءة قطاعات إضافية (مثل القطاع 1 في MIFARE) وسجل البيانات.
- قارن أداء قارئ USB مع هاتف NFC (السرعة، التفاصيل المقروءة).

مثال للإجابة:

- **البيانات**:
  - UID: 04A1B2C3
  - نوع الرقاقة: NTAG213
  - التردد: HF
  - الاستخدام: ملصق NFC للتجربة
  - نتيجة الكتابة: كتبت "MyRFIDTest2025" بنجاح
  - اختبار الجهاز الآخر: النص ظهر في NFC Tools PC كنص NDEF، متطابق مع الهاتف
  - لقطات شاشة: [NFC Tools: قراءة/كتابة]، [NFC Tools PC: نص NDEF]
- **الفقرة**: "استخدمت NFC Tools لقراءة ملصق HF (NTAG213) مع UID: 04A1B2C3، وهو ملصق للتجربة. قرأت البيانات، ثم كتبت نص ‘MyRFIDTest2025’ بنجاح. اختبرت الرقاقة بقارئ ACR122U باستخدام NFC Tools PC، وأظهر النص كنص NDEF، متطابقًا مع قراءة الهاتف. الكتابة كانت ممكنة لأن NTAG213 غير محمية. تغيير البيانات مفيد لتخصيص الملصقات، مثل إضافة بيانات مشروع. تعلمت أن قارئ USB يوفر قراءة أسرع وتفاصيل إضافية (مثل حجم الذاكرة)، لكن الهاتف أكثر سهولة. تنسيق NDEF يضمن التوافق بين الأجهزة."

صورة توضيحية:

- لقطات شاشة: NFC Tools (هاتف)، NFC Tools PC (قارئ USB).
- صورة: هاتف يقرأ ملصق NFC، قارئ USB مع رقاقة، تعليق: "اختبر البيانات على هاتف وقارئ USB."

1.13 ملخص الفصل

- RFID تستخدم موجات الراديو، مع رقائق (LF، HF، UHF).
- تتفوق على الباركود في النطاق والتخزين، لكنها أغلى.
- NFC هي RFID بتردد HF، للاتصال القريب (مثل الدفع).
- هيكلية MIFARE Classic تتيح الكتابة في قطاعات.

- دراسة حالة Zara تُظهر كفاءة RFID.
- التمرين يتيح قراءة UID، كتابة بيانات، واختبارها بجهاز آخر.

1.14 أسئلة مراجعة

- كيف يختلف نطاق RFID عن NFC؟
- لماذا تُستخدم NFC في الدفع؟
- ما الذي يُخزن في قطاع MIFARE Classic؟
- ماذا تعلمت من كتابة البيانات واختبارها بقارئ USB؟

1.15 موارد إضافية

- **فيديوهات**:
  - "كيف تعمل RFID؟" (youtube.com/rfid-how-it-works](#)).
  - "RFID مقابل الباركود" (youtube.com/rfid-vs-barcode](#)).
- **موقع**: rfid-guide.x.ai.
- **تطبيقات**: NFC Tools، RFID TagInfo.
- **برامج**: NFC Tools PC، LibNFC.

1.3 مكونات نظام RFID

- **الرقاقة**: تخزن UID أو بيانات، نشطة/سلبية.
- **القارئ**: يقرأ/يكتب البيانات.
- **البرمجيات**: تعالج البيانات.

مخطط تدفق:

[رقاقة RFID] <--- موجات راديو ---> [قارئ USB] <--- RFID/شبكة] <--- [برمجيات]

1.4 أنواع رقائق RFID

- **LF (125-134 كيلوهرتز)**: للحيوانات، الدخول.
- **HF (13.56 ميجاهرتز)**: NFC، النقل.
- **UHF (860-960 ميجاهرتز)**: المخزون، اللوجستيات.

مخطط MIFARE Classic: 16 قطاعًا، UID في القطاع 0، رسم ملون (أحمر: UID، أخضر: بيانات، أزرق: مفاتيح).

1.5 الفرق بين الرقائق القابلة للكتابة والقراءة فقط

- **القراءة فقط**: بيانات ثابتة.
- **القراءة/الكتابة**: تتيح التعديل.

1.6 مقارنة RFID مع الباركود

- **الآلية**: RFID (موجات راديو)، باركود (مسح بصري).

- **سعة التخزين**: RFID (كيلوبايتات)، باركود (أحرف).
- **النطاق**: RFID (حتى 15 مترًا)، باركود (سنتيمترات).
- **التكلفة**: RFID (مرتفعة)، باركود (منخفضة).

مخطط 1.2: يُظهر RFID (قراءة متعددة) مقابل باركود (قراءة فردية).

1.7 مقارنة RFID مع NFC

- **التردد**: RFID (LF، HF، UHF)، NFC (HF فقط).
- **النطاق**: RFID (حتى 15 مترًا)، NFC (حتى 10 سم).
- **الاتصال**: RFID (أحادي/ثنائي محدود)، NFC (ثنائي، 3 أوضاع: قراءة/كتابة، Peer-to-Peer، محاكاة).
- **التطبيقات**: RFID (مخزون، دخول)، NFC (دفع، ملصقات).

مخطط 1.3: يُظهر RFID (مستودع، بطاقة دخول) مقابل NFC (هاتف يقرأ ملصق، دفع).

1.8 شرح التشفير في RFID *(قسم جديد)*

التشفير في RFID يُستخدم لحماية البيانات المخزنة على الرقائق من الوصول غير المصرح به أو التزوير. إليك نظرة شاملة على التشفير في RFID:

- **1. لماذا التشفير؟**
  - رقائق RFID (مثل بطاقات الدخول أو الدفع) تحتوي على بيانات حساسة (مثل UID، أرقام حسابات).
  - بدون تشفير، يمكن للمهاجمين قراءة أو تعديل البيانات باستخدام قارئ غير مصرح به.
  - التشفير يضمن:
    - **السرية**: البيانات لا تُقرأ إلا بمفتاح.
    - **النزاهة**: البيانات لا تُعدل دون إذن.
    - **المصادقة**: التحقق من هوية الرقاقة/القارئ.
- **2. أنواع التشفير في RFID**:
  - **تشفير بسيط (مثل MIFARE Classic)**:
    - يستخدم مفاتيح 48 بت (مفتاح A وB لكل قطاع).
    - مثال: بطاقة دخول مكتب تستخدم مفتاحًا لحماية القطاعات.
    - عيوب: عرضة للهجمات (مثل هجمات استخراج المفتاح) بسبب ضعف الخوارزمية (CRYPTO1).
  - **تشفير متقدم (مثل MIFARE DESFire)**:
    - يستخدم خوارزميات AES (128/256 بت) أو 3DES.
    - مثال: بطاقات الدفع NFC (مثل بطاقات المصرف) أو بطاقات النقل العام.
    - مزايا: مقاومة عالية للهجمات، تدعم مصادقة متبادلة.
  - **بدون تشفير**:
    - بعض الرقائق (مثل NTAG213 غير محمية) لا تستخدم تشفيرًا، مما يجعلها مناسبة للتطبيقات غير الحساسة (مثل ملصقات ذكية).
- **3. كيف يعمل التشفير؟**
  - **في MIFARE Classic**:
    - كل قطاع محمي بمفتاحين (A وB).
    - القارئ يرسل طلب مصادقة مع المفتاح، ثم يُسمح بالقراءة/الكتابة.
    - مثال: بطاقة دخول تتطلب مفتاح A لقراءة UID وبيانات القطاع 1.

- في **MIFARE DESFire**:
  - تستخدم جلسات تشفير (Session Encryption) مع مفاتيح AES.
  - المصادقة المتبادلة: الرقاقة والقارئ يتحققان من بعضهما.
  - مثال: بطاقة دفع تُشفر رقم الحساب أثناء الاتصال بالقارئ.

4. **التحديات**:
   - **الضعف الأمني**: MIFARE Classic كُسرت في 2008، مما أدى إلى تحسينات (مثل DESFire).
   - **التكلفة**: الرقائق المشفرة (مثل DESFire) أغلى من غير المشفرة.
   - **إدارة المفاتيح**: فقدان المفتاح يعني فقدان الوصول إلى البيانات.

5. **التطبيقات**:
   - **بطاقات الدخول**: تشفير بسيط لحماية UID وبيانات المستخدم.
   - **الدفع بدون تلامس**: تشفير AES لحماية بيانات الحساب.
   - **النقل العام**: تشفير لتتبع الرصيد ومنع التزوير.

رسم توضيحي (يُضاف في الكتاب):

- صورة تُظهر:
  - **MIFARE Classic**: رقاقة مع قفل رمزي (مفتاح 48 بت)، تعليق: "تشفير بسيط، عرضة للهجمات."
  - **MIFARE DESFire**: رقاقة مع قفل قوي (AES)، تعليق: "تشفير متقدم، أمان عالٍ."
  - تدفق بيانات: [رقاقة] --> [مفتاح تشفير] --> [قارئ] --> [بيانات مشفرة].
- تعليق: "التشفير يحمي بيانات RFID، لكن يتطلب إدارة مفاتيح دقيقة."

جدول مقارنة التشفير (يُضاف في الكتاب):

الرقاقة	التشفيرنوع	الأمانمستوى	التطبيقات
MIFAREClassic	CRYPTO1 48)(بت	(ضعيف)منخفض	تذاكردخول،
MIFAREDESFire	AES/3DES(128/256)	مرتفع	عامنقل دفع،
NTAG213 محمية)(غير	تشفيربدون	يوجدلا	تجاربذكية، ملصقات

أسئلة للتفكير:

- لماذا تُستخدم رقائق بدون تشفير في تطبيقات غير حساسة؟
- كيف يؤثر ضعف تشفير MIFARE Classic على الأمان؟

1.9 استخدامات RFID في الحياة اليومية

- التحكم بالوصول.
- إدارة المخزون.
- النقل العام.
- تتبع الحيوانات.

1.10 دراسة حالة: RFID في Zara

- ملصقات UHF لتتبع الملابس.
- قارئات محمولة لفحص المخزون.
- تغيير الأرقام لتحديث البيانات.

1.11 لماذا تغيير أرقام RFID؟

- إعادة تخصيص.
- إصلاح الأخطاء.
- التخصيص.

1.12 كيف تعمل RFID؟ (فيديو توضيحي)

- **فيديو 1**: "كيف تعمل RFID؟" (3 دقائق).
- **فيديو 2**: "RFID مقابل الباركود" (4 دقائق).
- **ملاحظة**: يمكن إضافة فيديو عن التشفير أو NFC لاحقًا.

1.13 تمرين عملي: قراءة UID، كتابة بيانات، واختبار بتطبيق ثالث *(تمرين معدل)*

الهدف: تعلم قراءة المعرف الفريد (UID) لرقاقة RFID، كتابة بيانات بسيطة (إذا كانت تدعم)، واختبار البيانات بتطبيق ثالث (مثل NXP TagInfo) لفهم RFID عمليًا. **الأدوات المطلوبة**:

- هاتف ذكي يدعم NFC (Android أو iPhone حديث).
- تطبيقات: NFC Tools، RFID TagInfo، NXP TagInfo (مجانية على Google Play/App Store).
- رقاقة RFID قابلة للكتابة (مثل NTAG213 أو MIFARE Classic غير محمية). للقراءة فقط، استخدم بطاقة دخول أو بطاقة بنكية NFC.
- دفتر ملاحظات أو تطبيق تدوين. **الخطوات**:
- **إعداد الأدوات**:
  - نزّل NFC Tools، RFID TagInfo، وNXP TagInfo على الهاتف، فعّل NFC (إعدادات → اتصالات → NFC).
- **تحديد رقاقة RFID**:
  - اختر رقاقة (ملصق NTAG213، بطاقة دخول، بطاقة مترو). للكتابة، تأكد من أنها قابلة للكتابة.
  - **تحذير أمان**: لا تكتب على بطاقات حساسة (مثل بطاقة عمل) لتجنب تعطيلها.
- **قراءة UID**:
  - افتح NFC Tools، اختر "Read".
  - ضع الرقاقة خلف الهاتف (مستشعر NFC).
  - سجّل: UID (مثل "04A1B2C3")، نوع الرقاقة (مثل NTAG213)، التردد (HF)، الاستخدام (مثل "ملصق NFC").
  - التقط لقطة شاشة.
- **كتابة بيانات بسيطة**:
  - في NFC Tools، تحقق من خيار "Write" (يظهر إذا كانت الرقاقة قابلة للكتابة).
  - اختر "Write" → "Add a Record" → "Text Record".
  - أدخل نصًا (مثل "MyRFIDTest2025").

- ضع الرقاقة خلف الهاتف واضغط "Write".
- إذا فشلت الكتابة، دوّن السبب (مثل "مطلوب مفتاح تشفير").
- **اختبار البيانات بتطبيق ثالث (NXP TagInfo)**:
  - افتح NXP TagInfo على الهاتف.
  - ضع الرقاقة خلف الهاتف لقراءتها.
  - تحقق مما إذا كُتب النص (مثل "MyRFIDTest2025") في قسم "NDEF Data" أو "Tag Content".
  - قارن البيانات مع NFC Tools وRFID TagInfo:
    - هل النص متطابق؟
    - هل يظهر تنسيق NDEF بشكل صحيح؟
    - هل هناك تفاصيل إضافية (مثل حجم الذاكرة أو تاريخ الكتابة)؟
  - سجّل: النص المقروء، التنسيق، أي اختلافات، ملاحظات عن واجهة NXP TagInfo.
  - التقط لقطة شاشة لواجهة NXP TagInfo.
- **تسجيل النتائج**:
  - دوّن:
    - **UID**: (مثل "04A1B2C3").
    - **نوع الرقاقة**: (مثل NTAG213).
    - **التردد**: (HF).
    - **الاستخدام**: (مثل "ملصق NFC للتجربة").
    - **نتيجة الكتابة**: (مثل "كتبت 'MyRFIDTest2025' بنجاح").
    - **اختبار التطبيق الثالث**: (مثل "النص ظهر في NXP TagInfo كنص NDEF، متطابق").
    - **لقطات شاشة**: واجهة NXP TagInfo، RFID TagInfo، NFC Tools.
- **تحليل النتائج**:
  - اكتب فقرة (150-200 كلمة):
    - وصف الرقاقة واستخدامها.
    - هل يمكن تغيير البيانات؟ لماذا؟
    - كيف يفيد تغيير البيانات؟
    - ما تعلمته من الكتابة واختبار البيانات بتطبيق ثالث (مثل توافق NDEF أو تفاصيل NXP TagInfo).
- **إرسال النتائج** (اختياري):
  - ارفع لقطات الشاشة وملاحظاتك إلى rfid-guide.x.ai (قسم "ملاحظاتي"). **معايير النجاح**:
- قراءة UID بنجاح باستخدام NFC Tools.
- محاولة كتابة بيانات (حتى لو فشلت) مع تسجيل السبب.
- اختبار البيانات بتطبيق NXP TagInfo مع مقارنة النتائج.
- فقرة تحليلية مع ثلاث لقطات شاشة (NFC Tools، RFID TagInfo، NXP TagInfo). **تحدي إضافي**:
- جرب كتابة رابط URL (مثل "https://x.ai") واختبره بـ NXP TagInfo (هل يظهر كرابط قابل للفتح؟).
- قارن واجهة NXP TagInfo مع RFID TagInfo (أيهما يعطي تفاصيل أكثر؟).
- إذا كانت الرقاقة MIFARE Classic، حاول قراءة معلومات التشفير (مثل وجود مفتاح) بـ NXP TagInfo.

مثال للإجابة:

- **البيانات**:
  - UID: 04A1B2C3
  - نوع الرقاقة: NTAG213
  - التردد: HF
  - الاستخدام: ملصق NFC للتجربة
  - نتيجة الكتابة: كتبت "MyRFIDTest2025" بنجاح
  - اختبار التطبيق الثالث: النص ظهر في NXP TagInfo كنص NDEF، متطابق مع NFC Tools
  - لقطات شاشة: [NFC Tools: قراءة/كتابة]، [RFID TagInfo: بيانات]، [NXP TagInfo: NDEF]
- **الفقرة**: "استخدمت NFC Tools لقراءة ملصق NTAG213) HF مع UID: 04A1B2C3)، وهو ملصق للتجربة. كتبت نص 'MyRFIDTest2025' بنجاح باستخدام Text Record. اختبرت البيانات بـ RFID TagInfo وNXP TagInfo، وأظهر النص كنص NDEF في كليهما، متطابقًا مع NFC Tools. NXP TagInfo أظهر تفاصيل إضافية مثل حجم الذاكرة (144 بايت). الكتابة كانت ممكنة لأن NTAG213 غير محمية. تغيير البيانات مفيد لتخصيص الملصقات، مثل إضافة رابط مشروع. تعلمت أن تنسيق NDEF يضمن التوافق بين التطبيقات، وأن NXP TagInfo يوفر واجهة أكثر تقنية من RFID TagInfo. التجربة أوضحت أهمية اختبار البيانات للتأكد من الدقة."

صورة توضيحية:

- لقطات شاشة: واجهات NFC Tools، RFID TagInfo، NXP TagInfo.
- صورة: هاتف يقرأ ملصق NFC، تعليق: "اختبر البيانات بتطبيقات متعددة (NFC Tools، NXP TagInfo)."

1.14 مخطط RFID/NFC (تفصيلي) *(قسم جديد للمخطط)*

لتوضيح عملية NFC كجزء من RFID، إليك مخططًا يُظهر تدفق البيانات في NFC مقارنةً بـ RFID العامة:

- **الوصف البصري (للصورة في الكتاب)**:
  - الصورة مقسمة إلى قسمين:
    - **RFID (عامة)**:
      - مشهد يُظهر قارئ UHF يفحص صندوق مخزون (نطاق 15 مترًا)، تعليق: "RFID: نطاق طويل، قراءة متعددة."
      - مشهد آخر: قارئ HF يقرأ بطاقة دخول (نطاق 10 سم)، تعليق: "RFID HF: مشابه لـ NFC لكن أحادي الاتجاه."
      - تدفق البيانات: [رقاقة] --> [موجات راديو] --> [قارئ] --> [بيانات].
    - **NFC**:
      - مشهد يُظهر هاتفًا يقرأ ملصق NFC (نطاق 4sm)، تعليق: "NFC: قراءة/كتابة، نطاق قصير."
      - مشهد آخر: هاتفان يتبادلان بيانات (Peer-to-Peer)، تعليق: "NFC: اتصال ثنائي."
      - تدفق البيانات: [رقاقة/هاتف] <--> [موجات راديو] <--> [هاتف/قارئ] <--> [بيانات].
  - **الألوان**: أزرق لـ RFID (تنوع الترددات)، أخضر لـ NFC (سهولة الاستخدام).
  - **أيقونات**: موجات راديو لـ RFID، هاتف ذكي لـ NFC.
  - **التعليق**: "مخطط 1.4: NFC هي RFID بتردد HF، مع اتصال ثنائي وتكامل مع الهواتف."
- **تصميم ASCII لعملية NFC** (تمثيل نصي):

```
+----------------------------------------+
|            عملية NFC                   |
+----------------------------------------+
| [ملصق NFC]          [هاتف ذكي]          |
|  | UID: A1B2C3      | NFC Tools/NXP     |
|  | نص: Test2025     |                    |
|  v                 v                   |
| ~~~ موجات راديو (13.56 ميجاهرتز) ~~~    |
|  |                 |                   |
|  v                 v                   |
| [بيانات] <-------> [بيانات]             |
| - UID              - UID               |
| - نص NDEF           - نص NDEF           |
|                    - حجم الذاكرة          |
+----------------------------------------+
| مقارنة مع RFID العامة:                  |
| [رقاقة UHF]        [قارئ UHF]           |
|  | UID: B2C3D4      |                   |
|  v                 v                   |
| ~~~ موجات راديو (860-960 ميجاهرتز) ~~~ |
|  |                 |                   |
|  v                 v                   |
| [بيانات] --------> [بيانات]             |
| - UID              - UID               |
+----------------------------------------+
```

- شرح ASCII:
  - **الجزء العلوي (NFC)**: يُظهر هاتفًا يقرأ ملصق NFC (UID ونص NDEF)، مع اتصال ثنائي (<-->).
  - **الجزء السفلي (RFID)**: يُظهر قارئ UHF يقرأ رقاقة UID (فقط)، مع اتصال أحادي (-->).
  - **موجات راديو**: تُمثل بـ "~~~"، مع تحديد التردد.
  - **البيانات**: NFC يوفر تفاصيل أكثر (مثل نص NDEF وحجم الذاكرة) بسبب التكامل مع التطبيقات.
- **الدمج في الكتاب**:
  - الصورة الملونة (مصممة بـ Adobe Illustrator) تُضاف تحت عنوان "مخطط 1.4".
  - تعليق: "يوضح المخطط كيف تتيح NFC اتصالًا ثنائيًا مقارنةً بـ RFID العامة."

1.15 ملخص الفصل

- RFID تستخدم موجات الراديو، مع رقائق (LF، HF، UHF).
- تتفوق على الباركود في النطاق والتخزين، وNFC هي RFID بتردد HF.
- التشفير (مثل AES في MIFARE DESFire) يحمي البيانات.
- هيكلية MIFARE Classic تتيح الكتابة.
- دراسة حالة Zara تُظهر كفاءة RFID.
- التمرين يتيح قراءة UID، كتابة بيانات، واختبارها بتطبيق NXP TagInfo.

1.16 أسئلة مراجعة

- كيف يختلف تشفير MIFARE Classic عن MIFARE DESFire؟
- لماذا تُستخدم NFC في الدفع بدلًا من UHF RFID؟
- ماذا تعلمت من اختبار البيانات بتطبيق NXP TagInfo؟
- كيف يساعد تنسيق NDEF في توافق NFC؟

1.17 موارد إضافية

- **فيديوهات**:
  - "كيف تعمل RFID؟" (youtube.com/rfid-how-it-works (#)).
  - "RFID مقابل الباركود" (youtube.com/rfid-vs-barcode (#)).
- **موقع**: rfid-guide.x.ai.
- **تطبيقات**: NXP TagInfo، RFID TagInfo، NFC Tools.
- **برامج**: LibNFC.

1.8 شرح التشفير في RFID

- **أنواع التشفير**:
  - MIFARE Classic: CRYPTO1 (48 بت)، ضعيف.
  - MIFARE DESFire: AES/3DES (128/256 بت)، قوي.
  - NTAG213 (غير محمية): بدون تشفير.
- **التطبيقات**: دخول، دفع، نقل عام.
- **التحديات**: ضعف MIFARE Classic، تكلفة DESFire، إدارة المفاتيح.

رسم توضيحي: MIFARE Classic (قفل بسيط) مقابل DESFire (قفل قوي).

1.9 شرح هجمات RFID الأمنية *(قسم جديد)*

رقائق RFID عرضة للهجمات إذا لم تُصمم بحماية كافية. إليك نظرة على الهجمات الأمنية، أمثلتها، وكيفية الحماية:

- **1. أنواع الهجمات**:
  - **التنصت (Eavesdropping)**:
    - المهاجم يعترض موجات الراديو بين الرقاقة والقارئ لسرقة البيانات (مثل UID أو بيانات غير مشفرة).
    - مثال: قراءة UID من بطاقة دخول غير مشفرة بقارئ غير مصرح به.
    - عرضة: رقائق بدون تشفير (مثل NTAG213 غير محمية) أو UHF (نطاق طويل).
  - **استنساخ (Cloning)**:
    - المهاجم ينسخ بيانات الرقاقة (مثل UID) إلى رقاقة أخرى لخداع النظام.
    - مثال: استنساخ بطاقة دخول MIFARE Classic باستخدام قارئ مثل Proxmark3.
    - عرضة: MIFARE Classic (تشفير ضعيف).
  - **هجمات استخراج المفتاح (Key Cracking)**:
    - المهاجم يكسر مفاتيح التشفير (مثل مفتاح A/B في MIFARE Classic) باستخدام أدوات مثل Proxmark3.
    - مثال: كسر مفتاح MIFARE Classic في ثوانٍ بسبب ضعف CRYPTO1.

- عرضة: MIFARE Classic.
- **هجمات التلاعب (Data Tampering)**:
  - المهاجم يعدل بيانات الرقاقة (مثل رصيد بطاقة نقل) إذا كانت غير محمية.
  - مثال: تغيير رصيد بطاقة مترو غير مشفرة.
  - عرضة: رقائق قابلة للكتابة بدون تشفير.
- **هجمات الحرمان من الخدمة (DoS)**:
  - المهاجم يعطل الرقاقة أو القارئ (مثل تشويش موجات الراديو).
  - مثال: إرسال إشارات راديو لتعطيل قارئ دخول.

- **2. أمثلة واقعية**:
  - **2008: كسر MIFARE Classic**: باحثون هولنديون كشفوا ضعف CRYPTO1، مما سمح باستنساخ بطاقات النقل.
  - **2015: سرقة بيانات NFC**: هجمات تنصت على بطاقات دفع غير محمية جيدًا في أماكن مزدحمة.
  - **2023: هجمات UHF**: استنساخ ملصقات مخزون في مستودعات بسبب نطاقها الطويل.
- **3. كيفية الحماية**:
  - **استخدام تشفير قوي**:
    - اختر رقائق مثل MIFARE DESFire (AES/3DES) بدلًا من MIFARE Classic.
    - مثال: بطاقات الدفع تستخدم AES لمنع التنصت.
  - **تقليل النطاق**:
    - استخدم NFC أو HF (نطاق قصير) بدلًا من UHF لتطبيقات حساسة.
    - مثال: NFC في الدفع يقلل من مخاطر التنصت.
  - **إدارة المفاتيح**:
    - استخدم مفاتيح فريدة لكل رقاقة، وغيّرها دوريًا.
    - مثال: أنظمة الدخول تستخدم مفاتيح ديناميكية.
  - **حماية مادية**:
    - استخدم أغلفة حماية RFID (مثل محافظ مانعة للإشارة) لمنع القراءة غير المصرح بها.
    - مثال: محافظ لبطاقات الدفع NFC.
  - **تحديث الأنظمة**:
    - استبدل رقائق MIFARE Classic بـ DESFire أو رقائق أحدث.
    - مثال: مدن مثل لندن حولت بطاقات النقل إلى DESFire.
- **4. تأثير الهجمات**:
  - **مالي**: سرقة أموال من بطاقات دفع أو تزوير بطاقات نقل.
  - **أمني**: اختراق أنظمة الدخول (مثل مكاتب أو فنادق).
  - **تشغيلي**: تعطيل إدارة المخزون في المستودعات.

رسم توضيحي (يُضاف في الكتاب):

- صورة تُظهر:
  - **هجوم**: مهاجم يستخدم قارئ غير مصرح به لاعتراض بيانات من بطاقة RFID (مثل UID).
  - **حماية**: بطاقة DESFire مع رمز قفل AES، ومحفظة مانعة للإشارة.
  - تدفق: [رقاقة ضعيفة] --> [هجوم: تنصت/استنساخ] مقابل [رقاقة DESFire] --> [حماية: تشفير AES].
- تعليق: "الهجمات الأمنية تهدد RFID غير المحمية، لكن التشفير القوي يقلل المخاطر."

جدول مقارنة الهجمات (يُضاف في الكتاب):

الهجوم	الوصف	المعرضةالرقائق	الحماية
التنصت	البياناتاعتراض	NTAG213UHF،	قصيرنطاق AES، تشفير
الاستنساخ	أخرىرقاقة إلى البيانات نسخ	MIFAREClassic	ديناميكيةمفاتيح DESFire،
المفتاحاستخراج	التشفيرمفاتيح كسر	MIFAREClassic	AES/3DES
بالبياناتالتلاعب	البياناتتعديل	محميةغير رقائق	الكتابةقفل تشفير،
الخدمةمن الحرمان	الرقاقة/القارئتعطيل	الرقائقجميع	احتياطيةأنظمة التشويش، كشف

أسئلة للتفكير:

- لماذا تكون رقائق UHF أكثر عرضة للتنصت من NFC؟
- كيف تساعد محافظ الحماية في تقليل مخاطر الهجمات؟

1.10 استخدامات RFID في الحياة اليومية

- التحكم بالوصول.
- إدارة المخزون.
- النقل العام.
- تتبع الحيوانات.

1.11 دراسة حالة: RFID في Zara

- ملصقات UHF لتتبع الملابس.
- قارئات محمولة لفحص المخزون.
- تغيير الأرقام لتحديث البيانات.

1.12 لماذا تغيير أرقام RFID؟

- إعادة تخصيص.
- إصلاح الأخطاء.
- التخصيص.

1.13 كيف تعمل RFID؟ (فيديو توضيحي)

- **فيديو 1**: "كيف تعمل RFID؟" (3 دقائق).
- **فيديو 2**: "RFID مقابل الباركود" (4 دقائق).
- **ملاحظة**: يمكن إضافة فيديو عن هجمات RFID لاحقًا.

1.14 تمرين عملي: قراءة UID، كتابة بيانات، واختبار بتطبيق ثالث وجهاز آخر *(تمرين معدل)*

الهدف: تعلم قراءة المعرف الفريد (UID) لرقاقة RFID، كتابة بيانات بسيطة (إذا كانت تدعم)، واختبار البيانات بتطبيق ثالث (NXP TagInfo) وجهاز آخر (هاتف ثانٍ أو قارئ USB) لفهم RFID عمليًا. **الأدوات المطلوبة**:

- هاتف ذكي يدعم NFC (Android أو iPhone حديث).
- تطبيقات: NXP TagInfo، RFID TagInfo، NFC Tools (مجانية على Google Play/App Store).
- رقاقة RFID قابلة للكتابة (مثل NTAG213 أو MIFARE Classic غير محمية). للقراءة فقط، استخدم بطاقة دخول أو بطاقة بنكية NFC.
- جهاز آخر: هاتف ثانٍ يدعم NFC، أو قارئ USB (مثل ACR122U) مع NFC Tools PC أو LibNFC.
- دفتر ملاحظات أو تطبيق تدوين. **الخطوات**:
- **إعداد الأدوات**:
  - نزّل NXP TagInfo، RFID TagInfo، NFC Tools، وNXP TagInfo على الهاتف الأول، فعّل NFC (إعدادات → اتصالات → NFC).
  - إذا كنت تستخدم هاتفًا ثانيًا، ثبّت NFC Tools أو NXP TagInfo عليه.
  - إذا كنت تستخدم قارئ USB، وصّله بالكمبيوتر، ثبّت التعريفات، ونزّل NFC Tools PC أو LibNFC (رابط في الملحقات).
- **تحديد رقاقة RFID**:
  - اختر رقاقة (ملصق NTAG213، بطاقة دخول، بطاقة مترو). للكتابة، تأكد من أنها قابلة للكتابة.
  - **تحذير أمان**: لا تكتب على بطاقات حساسة (مثل بطاقة عمل) لتجنب تعطيلها.
- **قراءة UID**:
  - افتح NFC Tools على الهاتف الأول، اختر "Read".
  - ضع الرقاقة خلف الهاتف.
  - سجّل: UID (مثل "04A1B2C3")، نوع الرقاقة (مثل NTAG213)، التردد (HF)، الاستخدام (مثل "ملصق NFC").
  - التقط لقطة شاشة.
- **كتابة بيانات بسيطة**:
  - في NFC Tools، تحقق من خيار "Write" (يظهر إذا كانت الرقاقة قابلة للكتابة).
  - اختر "Write" → "Add a Record" → "Text Record".
  - أدخل نصًا (مثل "MyRFIDTest2025").
  - ضع الرقاقة خلف الهاتف واضغط "Write".
  - إذا فشلت الكتابة، دوّن السبب (مثل "مطلوب مفتاح تشفير").
- **اختبار البيانات بتطبيق ثالث (NXP TagInfo)**:
  - افتح NXP TagInfo على الهاتف الأول.
  - ضع الرقاقة خلف الهاتف لقراءتها.
  - تحقق مما إذا كُتب النص (مثل "MyRFIDTest2025") في قسم "NDEF Data" أو "Tag Content".
  - قارن البيانات مع NFC Tools وRFID TagInfo (هل النص متطابق؟ هل هناك تفاصيل إضافية؟).
  - سجّل: النص المقروء، التنسيق (مثل NDEF)، ملاحظات عن واجهة NXP TagInfo.
  - التقط لقطة شاشة.
- **اختبار البيانات بجهاز آخر**:
  - **خيار 1: هاتف ثانٍ**:
    - افتح NFC Tools أو NXP TagInfo على هاتف ثانٍ.
    - ضع الرقاقة خلف الهاتف لقراءتها.
    - تحقق مما إذا ظهر النص (مثل "MyRFIDTest2025") كـ NDEF أو إشعار.

- قارن البيانات مع الهاتف الأول وNXP TagInfo.
- التقط لقطة شاشة.
- **خيار 2: قارئ USB**:
- وصّل قارئ USB (مثل ACR122U) بالكمبيوتر.
- افتح NFC Tools PC، ضع الرقاقة على القارئ، واختر "Read".
- تحقق مما إذا ظهر النص في قسم "Data" أو "NDEF Records".
- (اختياري) استخدم LibNFC لقراءة البيانات الخام (مثل القطاعات).
- قارن البيانات مع الهاتف الأول وNXP TagInfo.
- التقط لقطة شاشة.
- **التحليل**: سجّل أي اختلافات (مثل تنسيق البيانات، سرعة القراءة، تفاصيل إضافية).
- **تسجيل النتائج**:
- دوّن:
- **UID**: (مثل "04A1B2C3").
- **نوع الرقاقة**: (مثل NTAG213).
- **التردد**: (HF).
- **الاستخدام**: (مثل "ملصق NFC للتجربة").
- **نتيجة الكتابة**: (مثل "كتبت 'MyRFIDTest2025' بنجاح").
- **اختبار NXP TagInfo**: (مثل "النص ظهر كنص NDEF، مع حجم الذاكرة").
- **اختبار الجهاز الآخر**: (مثل "النص ظهر على هاتف ثانٍ، متطابق").
- **لقطات شاشة**: NFC Tools، RFID TagInfo، NXP TagInfo، جهاز آخر (هاتف ثانٍ أو NFC Tools PC).
- **تحليل النتائج**:
- اكتب فقرة (150-200 كلمة):
- وصف الرقاقة واستخدامها.
- هل يمكن تغيير البيانات؟ لماذا؟
- كيف يفيد تغيير البيانات؟
- ما تعلمته من اختبار البيانات بتطبيق ثالث وجهاز آخر (مثل توافق NDEF أو دقة الأجهزة).
- **إرسال النتائج** (اختياري):
- ارفع لقطات الشاشة وملاحظاتك إلى rfid-guide.x.ai (قسم "ملاحظاتي"). **معايير النجاح**:
- قراءة UID بنجاح باستخدام NFC Tools.
- محاولة كتابة بيانات (حتى لو فشلت) مع تسجيل السبب.
- اختبار البيانات بـ NXP TagInfo وجهاز آخر (هاتف ثانٍ أو قارئ USB) مع مقارنة النتائج.
- فقرة تحليلية مع أربع لقطات شاشة (NFC Tools، RFID TagInfo، NXP TagInfo، جهاز آخر). **تحدي إضافي**:
- جرب كتابة رابط URL (مثل "https://x.ai") واختبره بـ NXP TagInfo وجهاز آخر (هل يفتح الرابط؟).
- إذا استخدمت قارئ USB، قارن قراءة NFC Tools PC مع LibNFC (أيهما يعطي تفاصيل أكثر؟).
- إذا كانت الرقاقة MIFARE Classic، تحقق من وجود تشفير بـ NXP TagInfo وسجّل النتائج.

مثال للإجابة:

- **البيانات**:
- UID: 04A1B2C3
- نوع الرقاقة: NTAG213

- التردد: HF
- الاستخدام: ملصق NFC للتجربة
- نتيجة الكتابة: كتبت "MyRFIDTest2025" بنجاح
- اختبار NXP TagInfo: النص ظهر كنص NDEF، مع حجم الذاكرة 144 بايت
- اختبار الجهاز الآخر: النص ظهر على هاتف ثانٍ كنص NDEF، متطابق
- لقطات شاشة: [NFC Tools: قراءة/كتابة]، [RFID TagInfo: بيانات]، [NXP TagInfo: NDEF]، [هاتف ثانٍ: نص]

- **الفقرة**: "استخدمت NFC Tools لقراءة ملصق NTAG213) HF) مع UID: 04A1B2C3، وهو ملصق للتجربة. كتبت نص ‘MyRFIDTest2025’ بنجاح. اختبرت البيانات بـ RFID TagInfo وNXP TagInfo، وأظهر النص كنص NDEF. NXP TagInfo أظهر تفاصيل إضافية مثل حجم الذاكرة. استخدمت هاتفًا ثانيًا للاختبار، وظهر النص متطابقًا. الكتابة كانت ممكنة لأن NTAG213 غير محمية. تغيير البيانات مفيد لتخصيص الملصقات، مثل إضافة رابط. تعلمت أن تنسيق NDEF يضمن التوافق، وNXP TagInfo يوفر واجهة تقنية، بينما الهاتف الثاني أكد دقة الكتابة. التجربة أوضحت أهمية التحقق من البيانات عبر أجهزة متعددة."

صورة توضيحية:

- لقطات شاشة: واجهات NXP TagInfo ،RFID TagInfo ،NFC Tools، هاتف ثانٍ أو NFC Tools PC.
- صورة: هاتف يقرأ ملصق NFC، قارئ USB (إن وجد)، تعليق: "اختبر البيانات بتطبيقات وأجهزة متعددة."

1.15 مخطط تدفق التشفير في RFID *(قسم جديد للمخطط)*

لتوضيح كيفية حماية البيانات في RFID باستخدام التشفير، إليك مخططًا يُظهر تدفق التشفير في رقاقة مثل MIFARE DESFire:

- **الوصف البصري (للصورة في الكتاب)**:
  - الصورة مقسمة إلى ثلاثة أجزاء:
    - **بدون تشفير (NTAG213)**:
      - مشهد: هاتف يقرأ ملصق NTAG213، البيانات (مثل نص) تُرسل مباشرة.
      - تعليق: "بدون تشفير، البيانات مكشوفة للتنصت."
      - تدفق: [رقاقة] --> [بيانات مكشوفة] --> [قارئ].
    - **تشفير بسيط (MIFARE Classic)**:
      - مشهد: قارئ يرسل مفتاح A لفتح قطاع في بطاقة دخول.
      - تعليق: "تشفير CRYPTO1 ضعيف، عرضة لاستخراج المفتاح."
      - تدفق: [رقاقة] --> [مفتاح A] --> [قارئ] --> [بيانات مشفرة].
    - **تشفير قوي (MIFARE DESFire)**:
      - مشهد: هاتف يقرأ بطاقة دفع، مع رمز قفل AES.
      - تعليق: "تشفير AES يحمي البيانات حتى في الاتصال."
      - تدفق: [رقاقة] --> [مصادقة AES] --> [قارئ] --> [بيانات مشفرة].
  - **الألوان**: أحمر لعدم التشفير (خطر)، أصفر لـ MIFARE Classic (ضعيف)، أخضر لـ DESFire (آمن).
  - **أيقونات**: قفل مفتوح (NTAG213)، قفل بسيط (MIFARE Classic)، قفل قوي (DESFire).
  - **التعليق**: "مخطط 1.5: التشفير القوي (مثل AES) يحمي بيانات RFID من الهجمات."
- **تصميم ASCII لتدفق التشفير** (تمثيل نصي):

```
+--------------------------------------------+
|          تدفق التشفير في RFID               |
+--------------------------------------------+
| 1. بدون تشفير (NTAG213)                     |
| [ملصق NTAG213]          [هاتف NFC]          |
|   | UID: A1B2C3          |                  |
|   | نص: Test2025         |                  |
|   v                      v                  |
| ~~~ موجات راديو ~~~                         |
|   |                      |                  |
|   v                      v                  |
| [بيانات مكشوفة] ----> [بيانات: Test2025]    |
+--------------------------------------------+
| 2. تشفير بسيط (MIFARE Classic)              |
| [بطاقة MIFARE]          [قارئ]              |
|   | UID: B2C3D4          |                  |
|   | مفتاح A: 48 بت      |                  |
|   v                      v                  |
| ~~~ موجات راديو ~~~                         |
|   | [مصادقة: مفتاح A] |                     |
|   v                      v                  |
| [بيانات مشفرة] -----> [بيانات مقروءة]       |
+--------------------------------------------+
| 3. تشفير قوي (MIFARE DESFire)               |
| [بطاقة DESFire]         [هاتف NFC]          |
|   | UID: C3D4E5          |                  |
|   | مفتاح AES: 128 بت  |                  |
|   v                      v                  |
| ~~~ موجات راديو ~~~                         |
|   | [مصادقة متبادلة: AES] |                 |
|   v                      v                  |
| [بيانات مشفرة] -----> [بيانات آمنة]         |
+--------------------------------------------+
```

- **شرح ASCII**:
  - **الجزء الأول (NTAG213)**: يُظهر بيانات مكشوفة تنتقل مباشرة (خطر التنصت).
  - **الجزء الثاني (MIFARE Classic)**: يُظهر مصادقة بمفتاح A، لكن التشفير ضعيف.
  - **الجزء الثالث (MIFARE DESFire)**: يُظهر مصادقة متبادلة بـ AES، مع بيانات آمنة.
  - **موجات راديو**: تُمثل بـ "~~~" لإيحاء الاتصال.
- **الدمج في الكتاب**:
  - الصورة الملونة تُضاف تحت عنوان "مخطط 1.5".
  - تعليق: "يوضح المخطط كيف يعزز التشفير القوي أمان بيانات RFID."

1.16 ملخص الفصل

- RFID تستخدم موجات الراديو، مع رقائق (LF، HF، UHF).
- تتفوق على الباركود، وNFC هي RFID بتردد HF.
- التشفير (مثل AES) يحمي البيانات، لكن الهجمات (مثل التنصت) تهدد الرقائق الضعيفة.
- هيكلية MIFARE Classic تتيح الكتابة.
- دراسة حالة Zara تُظهر كفاءة RFID.
- التمرين يتيح قراءة UID، كتابة بيانات، واختبارها بـ NXP TagInfo وجهاز آخر.

1.17 أسئلة مراجعة

- كيف تحمي رقائق MIFARE DESFire من هجمات الاستنساخ؟
- لماذا تُعتبر NFC أكثر أمانًا من UHF RFID؟
- ماذا تعلمت من اختبار البيانات بـ NXP TagInfo وجهاز آخر؟
- كيف يؤثر التشفير على أداء RFID؟

1.18 موارد إضافية

- **فيديوهات**:
  - "كيف تعمل RFID؟" youtube.com/rfid-how-it-works) (#)).
  - "RFID مقابل الباركود" youtube.com/rfid-vs-barcode) (#)).
- **موقع**: rfid-guide.x.ai.
- **تطبيقات**: NXP TagInfo، RFID TagInfo، NFC Tools.
- **برامج**: LibNFC، NFC Tools PC.

الفصل الثاني: فهم أرقام RFID

أهداف الفصل

- فهم ماهية أرقام RFID (UID، بيانات القطاعات، NDEF).
- استكشاف هيكلية رقائق RFID (MIFARE Classic، NTAG213، MIFARE DESFire).
- تعلم قراءة UID عمليًا باستخدام تطبيق NFC.
- استخدام أداة تفاعلية لمحاكاة هيكلية القطاعات.
- تحليل دور الأرقام في تطبيقات RFID (مثل الدخول، الدفع).

2.1 مقدمة إلى أرقام RFID

أرقام RFID هي البيانات المخزنة على رقاقة RFID، وتُستخدم لتحديد الهوية، تخزين المعلومات، أو تنفيذ وظائف (مثل فتح باب أو دفع مبلغ). تشمل الأرقام:

- **UID (Unique Identifier)**: المعرف الفريد للرقاقة، مثل رقم تسلسلي (مثل "04A1B2C3").
- **بيانات القطاعات**: معلومات مخصصة (مثل اسم المستخدم، رصيد بطاقة).
- **بيانات NDEF (NFC Data Exchange Format)**: تنسيق موحد لتخزين نصوص، روابط URL، أو بيانات أخرى في NFC.

لماذا الأرقام مهمة؟

- تمكّن الأنظمة من التعرف على الرقاقة (مثل بطاقة دخول).
- تتيح تخصيص التطبيقات (مثل كتابة رابط URL على ملصق NFC).
- تؤثر على الأمان (مثل حماية UID بتشفير).

مثال توضيحي:

- بطاقة دخول: UID يحدد المستخدم، بيانات القطاع تحدد الأذونات.
- ملصق NFC: يحتوي على رابط URL (مثل "https://x.ai") بتنسيق NDEF.

2.2 أنواع أرقام RFID

2.2.1 المعرف الفريد (UID)

- **التعريف**: رقم فريد مُبرمج مسبقًا في الرقاقة أثناء التصنيع.
- **الخصائص**:
  - غير قابل للتغيير في معظم الرقائق (مثل NTAG213، MIFARE Classic).
  - يتراوح طوله بين 4-10 بايت (مثل "04A1B2C3" لـ 4 بايت).
  - يُستخدم كمعرف أساسي في أنظمة التحكم بالوصول.
- **الأنواع**:
  - **UID ثابت**: موجود في معظم الرقائق (مثل NTAG213).
  - **UID عشوائي**: بعض رقائق NFC (مثل بطاقات الدفع) تولد UID عشوائي لكل جلسة لزيادة الأمان.
- **التطبيقات**:
  - تحديد بطاقة دخول في مبنى.
  - تتبع عنصر في مستودع.

2.2.2 بيانات القطاعات

- **التعريف**: بيانات مخصصة تُخزن في قطاعات/كتل الرقاقة.
- **الخصائص**:
  - تُنظم في قطاعات (Sectors) وكتل (Blocks) في رقائق مثل MIFARE Classic.
  - قابلة للكتابة إذا سمحت الرقاقة (مثل NTAG213، MIFARE غير محمية).
  - محمية بمفاتيح تشفير في الرقائق الآمنة (مثل MIFARE DESFire).
- **التطبيقات**:
  - تخزين رصيد بطاقة نقل عام.
  - حفظ بيانات المستخدم (مثل رقم الموظف).

2.2.3 بيانات NDEF

- **التعريف**: تنسيق موحد لتخزين البيانات في رقائق NFC (مثل NTAG213).
- **الخصائص**:
  - يدعم نصوص، روابط URL، جهات اتصال، أو أوامر (مثل فتح تطبيق).
  - متوافق مع معظم أجهزة NFC (مثل الهواتف الذكية).
  - يُخزن في الذاكرة القابلة للكتابة.
- **التطبيقات**:

- ملصق NFC يفتح موقع ويب.
- بطاقة ذكية تُشارك جهة اتصال.

جدول مقارنة:

النوع	الوصف	التطبيقات	الأمان
UID	للتغييرقابل غير فريد، معرف	تتبعالهوية، تحديد	يُشفرلم إذا مكشوفًا يكون قد
القطاعاتبيانات	كتلفي مخصصة بيانات	مستخدمبيانات رصيد،	وجدت)(إن بمفاتيح محمية
NDEFبيانات	موحدNFC تنسيق	أوامرنصوص، روابط،	الرقاقةحماية على يعتمد

2.3 هيكلية رقائق RFID

رقائق RFID تختلف في هيكليتها حسب النوع (MIFARE Classic، NTAG213، MIFARE DESFire). إليك شرحًا لهيكلية الرقائق مع مخططات توضيحية.

2.3.1 MIFARE Classic

- **الوصف**: رقاقة HF (13.56 ميجاهرتز)، تُستخدم في بطاقات الدخول والنقل.
- **الهيكلية**:
  - **الذاكرة**: 1 كيلوبايت (MIFARE Classic 1K) أو 4 كيلوبايت (4K).
  - **التنظيم**: 16 قطاعًا (Sectors)، كل قطاع يحتوي على 4 كتل (Blocks).
  - **كل كتلة**: 16 بايت.
  - **القطاع 0، الكتلة 0**: تحتوي على UID ومعلومات المصنع (غير قابلة للتغيير).
  - **كتلة المقطورة (Trailer Block)**: تحتوي على مفاتيح التشفير (مفتاح A وB) وإعدادات الوصول.
- **الأمان**:
  - محمية بمفاتيح CRYPTO1 (48 بت)، لكنها ضعيفة وكُسرت في 2008.
  - يجب معرفة المفتاح للقراءة/الكتابة في القطاعات.
- **مثال**:
  - بطاقة دخول: القطاع 1 يحتوي على اسم المستخدم ورقم الموظف، محمي بمفتاح A.

مخطط هيكلية MIFARE Classic (ASCII):

```
+------------------------------------------+
|       هيكلية MIFARE Classic 1K           |
+------------------------------------------+
| القطاع 0                                 |
|   الكتلة 0: [UID: 04A1B2C3 | بيانات المصنع] |
|   الكتلة 1: [بيانات]                      |
|   الكتلة 2: [بيانات]                      |
|   الكتلة 3: [مفتاح A | إعدادات | مفتاح B] |
+------------------------------------------+
| القطاع 1                                 |
|   الكتلة 0: [بيانات: اسم المستخدم]        |
|   الكتلة 1: [بيانات: رقم الموظف]          |
|   الكتلة 2: [بيانات]                      |
|   الكتلة 3: [مفتاح A | إعدادات | مفتاح B] |
+------------------------------------------+
| ... (حتى القطاع 15)                      |
+------------------------------------------+
```

- **شرح المخطط**:
- يُظهر القطاع 0 (UID وبيانات المصنع) والقطاع 1 (بيانات مخصصة).
- كتلة المقطورة تحتوي على مفاتيح التشفير.
- **الصورة في الكتاب**:
- رسم ملون: جدول يُظهر 16 قطاعًا (كل قطاع 4 كتل).
- ألوان: أحمر لـ UID، أخضر للبيانات، أزرق للمفاتيح.
- تعليق: "مخطط 2.1: هيكلية MIFARE Classic تُنظم البيانات في قطاعات وكتل، مع حماية بمفاتيح."

2.3.2 NTAG213

- **الوصف**: رقاقة HF) NFC)، تُستخدم في الملصقات الذكية.
- **الهيكلية**:
- **الذاكرة**: 144 بايت قابلة للكتابة (من الصفحة 4 إلى 39).
- **التنظيم**: 45 صفحة (Pages)، كل صفحة 4 بايت.
- **الصفحة 0-2**: UID وبيانات المصنع (غير قابلة للتغيير).
- **الصفحة 3**: إعدادات القفل (Lock Bits).
- **الصفحات 4-39**: بيانات المستخدم (مثل نص NDEF).
- **الصفحة 40-41**: كلمة مرور (إن وجدت) وإعدادات الحماية.
- **الأمان**:
- يمكن قفل الكتابة (Lock Bits) لمنع التعديل.
- اختياري: حماية بكلمة مرور.
- لا تشفير افتراضي، مما يجعلها عرضة للتنصت.
- **مثال**:
- ملصق NFC: يحتوي على رابط "https://x.ai" في الصفحات 4-10 بتنسيق NDEF.

مخطط هيكلية NTAG213 (ASCII):

```
+------------------------------------------+
|          هيكلية NTAG213                  |
+------------------------------------------+
| الصفحة 0: [UID: 04A1B2C3]               |
| الصفحة 1: [بيانات المصنع]               |
| الصفحة 2: [بيانات المصنع]               |
| الصفحة 3: [إعدادات القفل]               |
| الصفحة 4: [بيانات NDEF - جزء 1: نص]      |
| الصفحة 5: [بيانات NDEF - جزء 2: نص]      |
| ...                                      |
| الصفحة 39: [بيانات NDEF - نهاية: نص]     |
| الصفحة 40: [كلمة مرور]                  |
| الصفحة 41: [إعدادات الحماية]            |
+------------------------------------------+
```

- **شرح المخطط**:
  - يُظهر الصفحات المخصصة لـ UID، إعدادات القفل، وبيانات NDEF.
  - الصفحات 4-39 لتخزين بيانات المستخدم.
- **الصورة في الكتاب**:
  - رسم خطي: يُظهر 45 صفحة كجدول، مع تظليل الصفحات القابلة للكتابة.
  - ألوان: أحمر لـ UID، أخضر للبيانات، أصفر لإعدادات القفل.
  - تعليق: "مخطط 2.2: NTAG213 تُنظم البيانات في صفحات، مع تركيز على تنسيق NDEF."

2.3.3 MIFARE DESFire

- **الوصف**: رقاقة HF آمنة، تُستخدم في الدفع والنقل العام.
- **الهيكلية**:
  - **الذاكرة**: 2K، 4K، أو 8K بايت.
  - **التنظيم**: ملفات (Files) بدلًا من قطاعات/كتل.
  - **التطبيقات (Applications)**: كل تطبيق يحتوي على ملفات بيانات (مثل ملف للرصيد، ملف للتاريخ).
  - **UID**: مخزن في منطقة خاصة، محمي بتشفير.
  - **إعدادات الأمان**: مفاتيح AES/3DES لكل تطبيق.
- **الأمان**:
  - تشفير قوي (AES 128/256 بت أو 3DES).
  - مصادقة متبادلة بين الرقاقة والقارئ.
  - مقاومة لهجمات استخراج المفتاح.
- **مثال**:
  - بطاقة دفع: تحتوي على ملف للحساب وملف للسجل، محمية بـ AES.

مخطط هيكلية MIFARE DESFire (ASCII):

```
+------------------------------------------+
|        هيكلية MIFARE DESFire             |
+------------------------------------------+
| [UID: C3D4E5 | بيانات المصنع]           |
+------------------------------------------+
| التطبيق 0 (رئيسي)                        |
|   - ملف 0: [إعدادات الأمان]             |
|   - ملف 1: [مفاتيح AES]                 |
+------------------------------------------+
| التطبيق 1 (مثل الدفع)                    |
|   - ملف 0: [رصيد الحساب]                |
|   - ملف 1: [سجل المعاملات]              |
+------------------------------------------+
| التطبيق 2 (مثل النقل)                    |
|   - ملف 0: [رصيد التذكرة]               |
|   - ملف 1: [تاريخ السفر]                |
+------------------------------------------+
```

- **شرح المخطط**:
  - يُظهر تنظيم البيانات في تطبيقات وملفات.
  - UID محمي، والملفات مشفرة بـ AES.
- **الصورة في الكتاب**:
  - رسم شجري: يُظهر التطبيقات كفروع، والملفات كأوراق.
  - ألوان: أحمر لـ UID، أخضر للملفات، أزرق للمفاتيح.
  - تعليق: "مخطط 2.3: MIFARE DESFire تُنظم البيانات في تطبيقات آمنة بتشفير AES."

رسم توضيحي عام (للكتاب):

- صورة مقسمة:
  - **MIFARE Classic**: جدول قطاعات/كتل، مع قفل رمزي (تشفير ضعيف).
  - **NTAG213**: شريط صفحات، مع رمز NDEF.
  - **MIFARE DESFire**: شجرة تطبيقات/ملفات، مع قفل AES.
- تعليق: "مخطط 2.4: مقارنة هيكلية الرقائق تُظهر تنوع التنظيم والأمان."

2.4 كيف تُستخدم أرقام RFID؟

2.4.1 التحكم بالوصول

- **المثال**: بطاقة مكتب تستخدم UID لتحديد الموظف، وبيانات القطاع للأذونات.
- **الآلية**:
  - القارئ يقرأ UID ويطابقها مع قاعدة بيانات.
  - إذا كانت الرقاقة مشفرة، يُطلب مفتاح لقراءة بيانات القطاع.
- **الأمان**: يعتمد على تشفير الرقاقة (مثل DESFire للأمان العالي).

2.4.2 إدارة المخزون

- **المثال**: ملصقات UHF في مستودع Zara تُحدد المنتجات.

- **الآلية**:
    - UID يُربط بمعلومات المنتج في قاعدة بيانات.
    - بيانات إضافية (مثل تاريخ الإنتاج) تُخزن في القطاعات.
- **الأمان**: غالبًا بدون تشفير بسبب انخفاض الحساسية.

2.4.3 الدفع بدون تلامس

- **المثال**: بطاقة NFC تستخدم UID عشوائي وملفات مشفرة.
- **الآلية**:
    - البيانات تُنقل بتنسيق NDEF أو ملفات DESFire.
    - التشفير (مثل AES) يحمي رقم الحساب.
- **الأمان**: تشفير قوي ونطاق قصير.

2.4.4 النقل العام

- **المثال**: بطاقة مترو تخزن رصيدًا في قطاع/ملف.
- **الآلية**:
    - القارئ يكتب/يقرأ الرصيد في القطاعات.
    - UID يُربط بحساب المستخدم.
- **الأمان**: تشفير (مثل DESFire) لمنع التزوير.

دراسة حالة: بطاقة Oyster في لندن:

- رقاقة MIFARE DESFire.
- ملفات للرصيد وسجل السفر، مشفرة بـ AES.
- UID عشوائي لكل جلسة لزيادة الأمان.

2.5 الأدوات المستخدمة لقراءة/كتابة أرقام RFID

- **تطبيقات الهاتف**:
    - **NFC Tools**: قراءة/كتابة UID وبيانات NDEF.
    - **NXP TagInfo**: تحليل هيكلية الرقاقة (مثل القطاعات).
    - **RFID TagInfo**: عرض التفاصيل التقنية.
- **قارئات USB**:
    - **ACR122U**: قراءة/كتابة HF، متوافق مع NFC Tools PC.
    - **Proxmark3**: أداة متقدمة لتحليل التشفير والهجمات.
- **برمجيات الكمبيوتر**:
    - **NFC Tools PC**: واجهة بسيطة للقراءة/الكتابة.
    - **LibNFC**: مكتبة مفتوحة لتحليل البيانات الخام.

مقارنة الأدوات

الأداة	الاستخدام	المميزات	القيود
NFC Tools	قراءة/كتابة NDEF	سهل الاستخدام، مجاني	محدود في الرقائق المشفرة
NXP TagInfo	تحليل هيكلية الرقاقة	تفاصيل تقنية، مجاني	لا يكتب البيانات
ACR122U	قراءة/كتابة HF	دقيق، يدعم التشفير	يتطلب كمبيوتر
Proxmark3	تحليل متقدم، هجمات أمنية	قوي جدًا	مكلف، معقد

2.6 تمرين عملي: قراءة UID باستخدام تطبيق

الهدف: تعلم قراءة المعرف الفريد (UID) لرقاقة RFID باستخدام تطبيق NFC Tools، مع تسجيل التفاصيل وتحليل النتائج.

الأدوات المطلوبة:

- هاتف ذكي يدعم NFC (Android أو iPhone حديث).
- تطبيق NFC Tools (مجاني على Google Play/App Store).
- رقاقة RFID (مثل MIFARE Classic، NTAG213، بطاقة دخول، بطاقة بنكية NFC).
- دفتر ملاحظات أو تطبيق تدوين. **الخطوات**:
- **إعداد الأدوات**:
  - نزّل NFC Tools على الهاتف، فعّل NFC (إعدادات → اتصالات → NFC).
  - تأكد من شحن الهاتف ووجود إشارة NFC قوية.
- **تحديد رقاقة RFID**:
  - اختر رقاقة (ملصق NTAG213، بطاقة دخول، بطاقة مترو).
  - **تحذير أمان**: لا تكتب على بطاقات حساسة لتجنب تعطيلها.
- **قراءة UID**:
  - افتح NFC Tools، اختر "Read".
  - ضع الرقاقة خلف الهاتف (مستشعر NFC، عادةً في المنتصف أو أعلى).
  - انتظر حتى تظهر البيانات على الشاشة.
  - سجّل:
    - **UID**: (مثل "04A1B2C3").
    - **نوع الرقاقة**: (مثل MIFARE Classic، NTAG213).
    - **التردد**: (مثل HF).
    - **الاستخدام**: (مثل "ملصق NFC للتجربة" أو "بطاقة دخول").
  - التقط لقطة شاشة لواجهة NFC Tools.
- **تحليل البيانات**:
  - تحقق من طول UID (4 أو 7 بايت؟).
  - هل الرقاقة قابلة للكتابة؟ (يظهر خيار "Write" إذا كانت كذلك).
  - إذا كانت مشفرة (مثل MIFARE Classic)، هل ظهرت رسالة "مطلوب مفتاح"؟
- **تسجيل النتائج**:
  - دوّن:
    - **UID**.
    - **نوع الرقاقة**.
    - **التردد**.
    - **الاستخدام**.

- **ملاحظات**: (مثل "UID مكون من 4 بايت، الرقاقة غير مشفرة").
- **لقطة شاشة**: واجهة NFC Tools.
- **تحليل النتائج**:
  - اكتب فقرة (150-200 كلمة):
    - وصف الرقاقة واستخدامها.
    - هل كان UID متاحًا بسهولة؟ لماذا؟
    - كيف يمكن استخدام UID في تطبيق (مثل الدخول أو التتبع)؟
    - ما تعلمته من قراءة UID (مثل سهولة NFC Tools أو قيود التشفير).
- **إرسال النتائج** (اختياري):
  - ارفع لقطة الشاشة وملاحظاتك إلى rfid-guide.x.ai (قسم "ملاحظاتي"). **معايير النجاح**:
- قراءة UID بنجاح باستخدام NFC Tools.
- تسجيل التفاصيل (UID، نوع الرقاقة، التردد، الاستخدام).
- فقرة تحليلية مع لقطة شاشة. **تحدي إضافي**:
- جرب قراءة UID بتطبيق آخر (مثل NXP TagInfo) وقارن النتائج (هل يظهر تفاصيل إضافية؟).
- إذا كانت الرقاقة تدعم NDEF، اقرأ أي بيانات إضافية (مثل نص أو URL).
- إذا كانت الرقاقة مشفرة، دوّن سبب فشل قراءة البيانات الإضافية.

مثال للإجابة:

- **البيانات**:
  - UID: 04A1B2C3
  - نوع الرقاقة: NTAG213
  - التردد: HF
  - الاستخدام: ملصق NFC للتجربة
  - ملاحظات: UID مكون من 4 بايت، الرقاقة غير مشفرة
  - لقطة شاشة: [NFC Tools: UID وبيانات]
- **الفقرة**: "استخدمت NFC Tools لقراءة ملصق NTAG213 (HF) مع UID: 04A1B2C3، وهو ملصق للتجربة. القراءة كانت سهلة لأن الرقاقة غير مشفرة، وظهر UID مكونًا من 4 بايت. التطبيق أظهر أيضًا أن الرقاقة قابلة للكتابة (خيار Write متاح). يمكن استخدام UID لتتبع الملصق في نظام إدارة، مثل ربطه بمنتج في مخزون. تعلمت أن NFC Tools سهل الاستخدام للمبتدئين، لكنه لا يُظهر تفاصيل مثل هيكلية القطاعات. التجربة أوضحت أهمية UID كمعرف أساسي، لكن الأمان يعتمد على تشفير الرقاقة."

صورة توضيحية:

- لقطة شاشة: واجهة NFC Tools تُظهر UID.
- صورة: هاتف يقرأ ملصق NFC، تعليق: "قراءة UID باستخدام NFC Tools."

2.7 أداة تفاعلية: محاكاة هيكلية القطاعات

الوصف: أداة رقمية تفاعلية (متوفرة في rfid-guide.x.ai) تتيح للقارئ محاكاة هيكلية القطاعات في رقائق RFID (مثل MIFARE Classic وNTAG213) لفهم تنظيم البيانات. **الهدف**:

- تصور هيكلية الرقاقة (قطاعات/كتل أو صفحات).
- محاكاة قراءة/كتابة البيانات.
- فهم تأثير التشفير على الوصول. **مكونات الأداة**:

- **واجهة المستخدم**:
  - لوحة تحكم رقمية تُظهر هيكلية الرقاقة:
    - **MIFARE Classic**: جدول 16 قطاعًا، 4 كتل لكل قطاع.
    - **NTAG213**: شريط 45 صفحة.
    - **MIFARE DESFire**: شجرة تطبيقات/ملفات.
  - أزرار تفاعلية: "قراءة"، "كتابة"، "إعدادات التشفير".
- **محاكاة القراءة**:
  - اختر رقاقة (مثل MIFARE Classic).
  - انقر على القطاع 0، الكتلة 0 لعرض UID (مثل "04A1B2C3").
  - إذا كان القطاع مشفرًا، تظهر رسالة "مطلوب مفتاح".
- **محاكاة الكتابة**:
  - اختر قطاعًا/صفحة قابلة للكتابة (مثل الصفحة 4 في NTAG213).
  - أدخل نصًا (مثل "Test2025") أو URL.
  - انقر "كتابة" لمحاكاة التخزين، مع عرض تنسيق NDEF.
- **محاكاة التشفير**:
  - أدخل مفتاحًا وهميًا (مثل مفتاح A لـ MIFARE Classic).
  - إذا كان المفتاح صحيحًا، يُسمح بالقراءة/الكتابة.
  - إذا كان خاطئًا، تظهر رسالة "فشل المصادقة".
- **لوحة المعلومات**:
  - تُظهر تفاصيل الرقاقة (UID، نوع، تردد، حجم الذاكرة).
  - رسم بياني: يُظهر القطاعات المستخدمة مقابل الخالية. **كيفية الاستخدام**:
- **الخطوة 1**: افتح rfid-guide.x.ai، انتقل إلى قسم "محاكاة RFID".
- **الخطوة 2**: اختر نوع الرقاقة (MIFARE Classic، NTAG213، DESFire).
- **الخطوة 3**: جرّب قراءة UID (انقر على القطاع 0 أو الصفحة 0).
- **الخطوة 4**: جرّب كتابة نص في قطاع/صفحة (مثل "Test2025").
- **الخطوة 5**: أدخل مفتاح تشفير وهمي لمحاكاة الوصول إلى قطاع مشفر.
- **الخطوة 6**: راجع لو personally analyzed content from the web and X posts to ensure the simulation reflects real-world RFID structures (e.g., MIFARE Classic sector layout).

مثال سيناريو:

- اختر MIFARE Classic.
- انقر على القطاع 0، الكتلة 0: يظهر UID "04A1B2C3".
- حاول قراءة القطاع 1: تظهر رسالة "مطلوب مفتاح A".
- أدخل مفتاح وهمي "FFFFFFFFFFFF" (افتراضي): يُسمح بالقراءة.
- اكتب نص "Employee123" في الكتلة 0، القطاع 1.
- لوحة المعلومات: تُظهر أن القطاع 1 مستخدم بنسبة 25%. **الصورة في الكتاب**:
- لقطة شاشة لواجهة الأداة تُظهر جدول MIFARE Classic (16 قطاعًا).
- تعليق: "مخطط 2.5: الأداة التفاعلية تُحاكي هيكلية الرقائق، مع محاكاة القراءة/الكتابة." **فوائد الأداة**:
- تبسيط فهم هيكلية القطاعات.
- تعليم تأثير التشفير على الوصول.
- تمكين التجربة دون الحاجة إلى أجهزة حقيقية. **تحدي إضافي**:
- جرّب محاكاة كتابة رابط URL في NTAG213 وتحقق من تنسيق NDEF.
- قارن واجهة MIFARE Classic مع DESFire في الأداة (أيهما أكثر تعقيدًا؟).

2.8 التحديات في التعامل مع أرقام RFID

- **الأمان:**
  - UID مكشوف في الرقائق غير المشفرة (مثل NTAG213)، مما يسهل التنصت.
  - MIFARE Classic عرضة لاستنساخ بسبب ضعف CRYPTO1.
- **التوافق:**
  - ليست كل الأجهزة تدعم قراءة جميع أنواع الرقائق (مثل UHF تتطلب قارئات مخصصة).
  - تنسيق NDEF قد لا يُقرأ بشكل صحيح في بعض التطبيقات.
- **إدارة البيانات:**
  - الكتابة المتكررة قد تؤدي إلى أخطاء في الرقائق القديمة.
  - إدارة المفاتيح معقدة في الرقائق المشفرة.
- **التكلفة:**
  - رقائق آمنة مثل MIFARE DESFire أغلى من NTAG213.
  - قارئات متقدمة (مثل Proxmark3) مكلفة.

حلول مقترحة:

- استخدام رقائق آمنة (مثل DESFire) للتطبيقات الحساسة.
- اختبار التوافق قبل النشر (مثل اختبار NDEF على أجهزة متعددة).
- الاحتفاظ بنسخ احتياطية للمفاتيح في أنظمة مشفرة.

2.9 دراسات حالة متقدمة

2.9.1 RFID في المستشفيات

- **السيناريو:** تتبع المعدات الطبية باستخدام ملصقات NTAG213.
- **الأرقام:**
  - UID يُربط بمعرف المعدة في قاعدة بيانات.
  - بيانات NDEF تُخزن موقع المعدة (مثل "غرفة 305").
- **التحديات:** التوافق مع أجهزة NFC المتنوعة.

2.9.2 NFC في التسويق

- **السيناريو:** ملصقات NFC على منتجات تشير إلى موقع ويب.
- **الأرقام:**
  - UID لتتبع الملصق.
  - NDEF يحتوي على URL (مثل "https://brand.com").
- **التحديات:** ضمان قراءة NDEF على جميع الهواتف.

2.10 ملخص الفصل

- أرقام RFID (UID، بيانات القطاعات، NDEF) هي جوهر عمل الرقائق.
- هيكلية الرقائق (MIFARE Classic، NTAG213، DESFire) تختلف في التنظيم والأمان.
- قراءة UID عملية بسيطة باستخدام NFC Tools، لكن التشفير قد يحد من الوصول.

- الأداة التفاعلية تُحاكي هيكلية القطاعات، مما يسهل التعلم.
- التطبيقات تشمل الدخول، المخزون، الدفع، والنقل، مع تحديات الأمان والتوافق.

2.11 أسئلة مراجعة

- ما الفرق بين UID وبيانات القطاعات؟
- كيف تُنظم البيانات في MIFARE Classic مقارنةً بـ NTAG213؟
- لماذا تُستخدم MIFARE DESFire في الدفع؟
- ماذا تعلمت من قراءة UID باستخدام NFC Tools؟
- كيف تساعد الأداة التفاعلية في فهم هيكلية الرقائق؟

2.12 موارد إضافية

- **فيديوهات**:
  - "فهم هيكلية MIFARE Classic" (youtube.com/mifare-structure (#)).
  - "قراءة UID باستخدام NFC Tools" (youtube.com/nfc-tools-uid (#)).
- **موقع**: rfid-guide.x.ai.
- **تطبيقات**: NFC Tools، NXP TagInfo، RFID TagInfo.
- **أداة تفاعلية**: rfid-guide.x.ai/simulator.

2.3 هيكلية رقائق RFID *(القسم الرئيسي)*

رقائق RFID تختلف في هيكليتها حسب النوع والتطبيق، مما يؤثر على كيفية تخزين الأرقام (مثل UID وبيانات القطاعات) وإدارتها. هذا القسم يشرح هيكلية ثلاث رقائق شائعة: **NTAG213**، **MIFARE Classic**، و**MIFARE DESFire**، مع مخططات توضيحية، أمثلة عملية، وتحليل الأمان.

2.3.1 MIFARE Classic

- **الوصف**: رقاقة HF (13.56 ميجاهرتز) تُستخدم في بطاقات الدخول، النقل العام، والتذاكر. تُعتبر من أكثر الرقائق شيوعًا رغم ضعف تشفيرها.
- **الهيكلية**:
  - **الذاكرة**:
    - MIFARE Classic 1K: 1024 بايت (1 كيلوبايت).
    - MIFARE Classic 4K: 4096 بايت.
  - **التنظيم**:
    - 16 قطاعًا (Sectors) في 1K، 40 قطاعًا في 4K.
    - كل قطاع يحتوي على 4 كتل (Blocks)، كل كتلة 16 بايت.
    - **القطاع 0، الكتلة 0**: تحتوي على UID (4 أو 7 بايت) وبيانات المصنع (غير قابلة للتغيير).
    - **الكتل 0-2**: بيانات المستخدم (مثل اسم، رقم موظف).
    - **الكتلة 3 (المقطورة)**: تحتوي على:
      - مفتاح A (6 بايت).
      - إعدادات الوصول (Access Bits، 4 بايت).
      - مفتاح B (6 بايت).
  - **إعدادات الوصول**:
    - تُحدد ما إذا كان القطاع قابلًا للقراءة/الكتابة.

- مثال: قد يسمح مفتاح A بالقراءة فقط، ومفتاح B بالكتابة.
- **الأمان**:
  - تستخدم تشفير CRYPTO1 (48 بت)، وهو ضعيف وكُسر في 2008.
  - عرضة لهجمات استخراج المفتاح باستخدام أدوات مثل Proxmark3.
  - المفاتيح الافتراضية (مثل "FFFFFFFFFFFF") تُستخدم في الرقائق غير المُهيأة، مما يزيد المخاطر.
- **مثال عملي**:
  - بطاقة دخول مكتب:
    - القطاع 0، الكتلة 0: UID "04A1B2C3".
    - القطاع 1، الكتلة 0: اسم المستخدم "John Doe".
    - القطاع 1، الكتلة 1: رقم الموظف "12345".
    - القطاع 1، الكتلة 3: مفتاح A وإعدادات تمنع الكتابة بدون مفتاح B.
- **التحديات**:
  - ضعف التشفير يجعلها غير مناسبة لتطبيقات حساسة (مثل الدفع).
  - إدارة المفاتيح معقدة إذا كانت فريدة لكل قطاع.

مخطط هيكلية MIFARE Classic (ASCII):

```
+------------------------------------------+
|       هيكلية MIFARE Classic 1K          |
+------------------------------------------+
| القطاع 0                                 |
|   الكتلة 0: [UID: 04A1B2C3 | بيانات مصنع] |
|   الكتلة 1: [بيانات]                     |
|   الكتلة 2: [بيانات]                     |
|   الكتلة 3: [مفتاح A | مفتاح | إعدادات B] |
+------------------------------------------+
| القطاع 1                                 |
|   الكتلة 0: [بيانات: John Doe]           |
|   الكتلة 1: [بيانات: 12345]              |
|   الكتلة 2: [بيانات]                     |
|   الكتلة 3: [مفتاح A | مفتاح | إعدادات B] |
+------------------------------------------+
| ... (حتى القطاع 15)                      |
+------------------------------------------+
```

- **شرح المخطط**:
  - يُظهر القطاع 0 (UID) والقطاع 1 (بيانات مخصصة).
  - كتلة المقطورة (الكتلة 3) تحدد الأمان.
- **الصورة في الكتاب**:
  - جدول ملون: 16 قطاعًا، كل قطاع 4 كتل.
  - ألوان: أحمر (UID)، أخضر (بيانات)، أزرق (مفاتيح).
  - تعليق: "مخطط 2.1: هيكلية MIFARE Classic تُنظم البيانات في قطاعات، مع حماية ضعيفة."

2.3.2 NTAG213

- **الوصف**: رقاقة HF (NFC) تُستخدم في الملصقات الذكية، مثل ملصقات التسويق أو التتبع.

- **الهيكلية**:
  - **الذاكرة**: 144 بايت قابلة للكتابة، 180 بايت إجمالي.
  - **التنظيم**:
    - 45 صفحة (Pages)، كل صفحة 4 بايت.
    - **الصفحة 0-2**: 7) UID بايت)، بيانات المصنع، غير قابلة للتغيير.
    - **الصفحة 3**: إعدادات القفل (Lock Bits) لمنع الكتابة.
    - **الصفحات 4-39**: بيانات المستخدم، غالبًا بتنسيق NDEF (مثل نص، URL).
    - **الصفحة 40-41**: كلمة مرور (اختيارية) وإعدادات الحماية.
  - **إعدادات القفل**:
    - يمكن قفل الصفحات 4-39 لتصبح للقراءة فقط.
    - القفل دائم (لا يمكن إلغاؤه).
- **الأمان**:
  - لا تشفير افتراضي، مما يجعل البيانات مكشوفة للتنصت.
  - حماية بكلمة مرور اختيارية (32 بت)، لكنها ضعيفة مقارنة بـ AES.
  - مناسبة لتطبيقات غير حساسة (مثل ملصقات ذكية).
- **مثال عملي**:
  - ملصق NFC في متجر:
    - الصفحة 0: UID "04A1B2C3".
    - الصفحات 4-10: رابط "https://brand.com" بتنسيق NDEF.
    - الصفحة 3: قفل لمنع التعديل.
- **التحديات**:
  - حجم الذاكرة الصغير (144 بايت) يحد من البيانات.
  - عدم وجود تشفير قوي يجعلها غير مناسبة للدفع.

مخطط هيكلية NTAG213 (ASCII):

```
+------------------------------------------+
|          هيكلية NTAG213                 |
+------------------------------------------+
| 0 الصفحة: [UID: 04A1B2C3]               |
| [بيانات المصنع] :1 الصفحة              |
| [بيانات المصنع] :2 الصفحة              |
| [إعدادات القفل] :3 الصفحة            |
| 4 الصفحة: [NDEF: https://brand.com - 1]   |
| 5 الصفحة: [NDEF: https://brand.com - 2]   |
| ...                                        |
| 39 الصفحة: [NDEF: نهاية]              |
| [كلمة مرور] :40 الصفحة                |
| [إعدادات الحماية] :41 الصفحة        |
+------------------------------------------+
```

- **شرح المخطط**:
  - يُظهر UID (الصفحة 0) وبيانات NDEF (الصفحات 4-39).
  - إعدادات القفل تمنع التعديل.
- **الصورة في الكتاب**:
  - شريط خطي: 45 صفحة، مع تظليل الصفحات القابلة للكتابة.
  - ألوان: أحمر (UID)، أخضر (NDEF)، أصفر (قفل).
  - تعليق: "مخطط 2.2: NTAG213 تُخزن بيانات NDEF في صفحات، مع حماية محدودة."

2.3.3 MIFARE DESFire

- **الوصف**: رقاقة HF آمنة تُستخدم في الدفع بدون تلامس، النقل العام، وأنظمة الدخول المتقدمة.
- **الهيكلية**:
  - **الذاكرة**: 2K، 4K، أو 8K بايت.
  - **التنظيم**:
    - **التطبيقات (Applications)**: تصل إلى 28 تطبيقًا، كل تطبيق يحتوي على ملفات (Files).
    - **ملفات البيانات**: تحتوي على بيانات مثل الرصيد، سجل المعاملات.
    - **UID**: مخزن في منطقة محمية، قابل للتكوين (ثابت أو عشوائي).
    - **إعدادات الأمان**: كل تطبيق محمي بمفتاح AES (128/256 بت) أو 3DES.
  - **إعدادات الوصول**:
    - مصادقة متبادلة بين الرقاقة والقارئ.
    - يمكن تخصيص أذونات لكل ملف (قراءة، كتابة، قراءة/كتابة).
- **الأمان**:
  - تشفير قوي (AES/3DES) يقاوم هجمات استخراج المفتاح.
  - UID عشوائي (اختياري) يمنع التتبع.
  - مناسبة لتطبيقات حساسة مثل الدفع.
- **مثال عملي**:
  - بطاقة دفع NFC:
    - التطبيق 1: ملف الرصيد "100 دولار".
    - التطبيق 1: ملف سجل المعاملات.
    - التطبيق 2: ملف بيانات المستخدم.
    - محمية بمفتاح AES 128 بت.
- **التحديات**:
  - التكلفة العالية مقارنة بـ MIFARE Classic.
  - التعقيد في إدارة التطبيقات والمفاتيح.

مخطط هيكلية MIFARE DESFire (ASCII):

```
+-----------------------------------------+
|        هيكلية MIFARE DESFire            |
+-----------------------------------------+
| [UID: C3D4E5 | بيانات المصنع]           |
+-----------------------------------------+
| التطبيق 0 (رئيسي)                       |
|   - ملف 0: [إعدادات الأمان]             |
|   - ملف 1: [مفاتيح AES]                 |
+-----------------------------------------+
| التطبيق 1 (الدفع)                       |
|   - ملف 0: [رصيد: 100 دولار]            |
|   - ملف 1: [سجل المعاملات]              |
+-----------------------------------------+
| التطبيق 2 (النقل)                       |
|   - ملف 0: [رصيد التذكرة]               |
|   - ملف 1: [تاريخ السفر]                |
+-----------------------------------------+
```

- **شرح المخطط**:
  - يُظهر تنظيم البيانات في تطبيقات وملفات.
  - UID والبيانات مشفرة بـ AES.
- **الصورة في الكتاب**:
  - شجرة: تطبيقات كفروع، ملفات كأوراق.
  - ألوان: أحمر (UID)، أخضر (ملفات)، أزرق (مفاتيح).
  - تعليق: "مخطط 2.3: MIFARE DESFire تُنظم البيانات في تطبيقات آمنة."

مقارنة هيكلية الرقائق:

الرقاقة	التنظيم	الذاكرة	الأمان	التطبيقات
MIFARE Classic	قطاعات/كتل	1K/4K بايت	CRYPTO1 (ضعيف)	دخول، تذاكر
NTAG213	صفحات	144 بايت	بدون تشفير/كلمة مرور	ملصقات ذكية
MIFARE DESFire	تطبيقات/ملفات	2K/4K/8K بايت	AES/3DES (قوي)	دفع، نقل عام

رسم توضيحي عام (للكتاب):

- صورة مقسمة:
  - MIFARE Classic: جدول قطاعات/كتل، قفل ضعيف.
  - NTAG213: شريط صفحات، رمز NDEF.
  - MIFARE DESFire: شجرة تطبيقات، قفل AES.
- تعليق: "مخطط 2.4: هيكليات الرقائق تُظهر تنوع التنظيم والأمان."

2.6 تمرين عملي: قراءة UID، كتابة NDEF، واختبار التشفير (*تمرين معدل*)

الهدف: تعلم قراءة UID، كتابة بيانات NDEF (مثل نص أو URL)، واختبار وجود تشفير في رقاقة RFID باستخدام تطبيق NFC Tools. **الأدوات المطلوبة**:

- هاتف ذكي يدعم NFC (Android أو iPhone حديث).
- تطبيقات: NFC Tools، NXP TagInfo (مجانية على Google Play/App Store).
- رقاقة RFID (مثل NTAG213 للكتابة، MIFARE Classic أو بطاقة دخول للتشفير).
- دفتر ملاحظات أو تطبيق تدوين. **الخطوات**:
- **إعداد الأدوات**:
  - نزّل NFC Tools وNXP TagInfo، فعّل NFC.
  - تأكد من شحن الهاتف.
- **تحديد رقاقة RFID**:
  - اختر رقاقة (NTAG213، MIFARE Classic، بطاقة دخول).
  - **تحذير أمان**: لا تكتب على بطاقات حساسة (مثل بطاقة دفع).
- **قراءة UID**:
  - افتح NFC Tools، اختر "Read".
  - ضع الرقاقة خلف الهاتف.
  - سجّل: UID (مثل "04A1B2C3")، نوع الرقاقة (مثل NTAG213)، التردد (HF)، الاستخدام.
  - التقط لقطة شاشة.
- **كتابة بيانات NDEF**:
  - في NFC Tools، تحقق من خيار "Write" (يظهر إذا كانت الرقاقة قابلة للكتابة).
  - اختر "Write" → "Add a Record" → "Text Record" أو "URL Record".
  - أدخل نصًا (مثل "MyRFIDTest2025") أو URL (مثل "https://x.ai").
  - ضع الرقاقة خلف الهاتف واضغط "Write".
  - سجّل: هل نجحت الكتابة؟ إذا فشلت، دوّن السبب (مثل "الرقاقة مقفلة").
  - التقط لقطة شاشة.
- **اختبار التشفير**:
  - افتح NXP TagInfo، ضع الرقاقة خلف الهاتف.
  - تحقق من وجود تشفير:
    - إذا كانت NTAG213: هل هناك كلمة مرور أو قفل؟ (عادةً لا تشفير).
    - إذا كانت MIFARE Classic: هل تظهر رسالة "مطلوب مفتاح" عند محاولة قراءة القطاعات؟
    - إذا كانت DESFire: هل تظهر رسالة "مصادقة AES مطلوبة"؟
  - سجّل: نوع التشفير (CRYPTO1، AES، بدون)، حالة الحماية (مقفلة، محمية بمفتاح).
  - التقط لقطة شاشة.
- **تسجيل النتائج**:

- دوّن:
  - **UID.**
  - **نوع الرقاقة.**
  - **التردد.**
  - **الاستخدام.**
  - **نتيجة الكتابة**: (مثل "كتبت URL بنجاح").
  - **نتيجة التشفير**: (مثل "بدون تشفير في NTAG213").
  - **لقطات شاشة**: NFC Tools (UID وNXP TagInfo، (NDEF (تشفير).
- **تحليل النتائج**:
  - اكتب فقرة (150-200 كلمة):
    - وصف الرقاقة واستخدامها.
    - هل نجحت كتابة NDEF؟ لماذا؟
    - هل وجدت تشفيرًا؟ كيف أثر على الوصول؟
    - ما تعلمته (مثل سهولة NDEF أو قيود التشفير).
- **إرسال النتائج** (اختياري):
  - ارفع لقطات الشاشة وملاحظاتك إلى rfid-guide.x.ai. **معايير النجاح**:
- قراءة UID بنجاح.
- كتابة بيانات NDEF (أو محاولة إذا كانت الرقاقة مقفلة).
- اختبار التشفير بـ NXP TagInfo.
- فقرة تحليلية مع ثلاث لقطات شاشة. **تحدي إضافي**:
- جرب كتابة URL واختبره على هاتف آخر (هل يفتح الرابط؟).
- إذا وجدت تشفيرًا، حاول تخمين نوعه (CRYPTO1، AES) بناءً على نوع الرقاقة.

مثال للإجابة:

- **البيانات**:
  - UID: 04A1B2C3
  - نوع الرقاقة: NTAG213
  - التردد: HF
  - الاستخدام: ملصق NFC
  - نتيجة الكتابة: كتبت "https://x.ai" بنجاح
  - نتيجة التشفير: بدون تشفير، الصفحات 4-39 مفتوحة
  - لقطات شاشة: [NFC Tools: UID]، [NFC Tools: NDEF]، [NXP TagInfo: بدون تشفير]
- **الفقرة**: "استخدمت NFC Tools لقراءة ملصق NTAG213) (HF) مع UID: 04A1B2C3. كتبت رابط 'https://x.ai' بتنسيق NDEF بنجاح في الصفحات 4-10. اختبرت التشفير بـ NXP TagInfo، وأظهر أن الرقاقة غير مشفرة ولا تحتوي على كلمة مرور. الكتابة نجحت لأن NTAG213 غير مقفلة. عدم وجود تشفير يجعلها عرضة للتنصت، لكنها مثالية لملصقات ذكية. تعلمت أن NDEF يضمن التوافق مع الهواتف، وNXP TagInfo يوفر تفاصيل تقنية مثل حجم الذاكرة (144 بايت). التجربة أوضحت أهمية اختبار التشفير لتحديد أمان الرقاقة."

صورة توضيحية:

- لقطات شاشة: NFC Tools (UID وNXP TagInfo، (NDEF (تشفير).
- صورة: هاتف يقرأ ملصق NFC، تعليق: "قراءة UID وكتابة NDEF مع اختبار التشفير."

2.7 أداة تفاعلية: محاكاة هيكلية القطاعات مع هجمات أمنية *(موسعة)*

الوصف: أداة رقمية تفاعلية (rfid-guide.x.ai) تُحاكي هيكلية رقائق RFID (MIFARE Classic، NTAG213، DESFire) وتتيح محاكاة هجمات أمنية لفهم نقاط الضعف. **الهدف**:

- تصور هيكلية الرقاقة (قطاعات، صفحات، تطبيقات).
- محاكاة قراءة/كتابة البيانات.
- محاكاة هجمات (مثل التنصت، استخراج المفتاح). **مكونات الأداة**:
- **واجهة المستخدم**:
  - لوحة تحكم تُظهر:
    - MIFARE Classic: جدول 16 قطاعًا.
    - NTAG213: شريط 45 صفحة.
    - DESFire: شجرة تطبيقات/ملفات.
  - أزرار: "قراءة"، "كتابة"، "إعدادات التشفير"، "محاكاة هجوم".
- **محاكاة القراءة/الكتابة**:
  - اختر رقاقة، انقر على القطاع 0 لقراءة UID.
  - اكتب نص (مثل "Test2025") في صفحة/قطاع.
  - إذا كان مشفرًا، أدخل مفتاحًا وهميًا.
- **محاكاة التشفير**:
  - لـ MIFARE Classic: أدخل مفتاح A (مثل "FFFFFFFFFFFF").
  - لـ DESFire: أدخل مفتاح AES وهمي.
  - تظهر رسائل مثل "مصادقة ناجحة" أو "فشل المصادقة".
- **محاكاة هجمات أمنية** *(ميزة جديدة)*:
  - **التنصت**:
    - اختر NTAG213، اقرأ الصفحة 4 (مثل URL).
    - الأداة تُظهر رسالة: "المهاجم اعترض البيانات: https://x.ai".
  - **استنساخ**:
    - اختر MIFARE Classic، انسخ UID وبيانات القطاع 1.
    - الأداة تُظهر: "تم استنساخ البيانات إلى رقاقة أخرى".
  - **استخراج المفتاح**:
    - اختر MIFARE Classic، حاول كسر مفتاح A.
    - الأداة تُظهر: "تم استخراج المفتاح في 5 ثوانٍ بسبب ضعف CRYPTO1".
  - **حماية DESFire**:
    - اختر DESFire، حاول استخراج مفتاح AES.
    - الأداة تُظهر: "فشل الهجوم، تشفير AES قوي".
- **لوحة المعلومات**:
  - تُظهر UID، نوع الرقاقة، حجم الذاكرة.
  - رسم بياني: نسبة القطاعات المستخدمة.
  - سجل الهجمات: (مثل "التنصت نجح على NTAG213"). **كيفية الاستخدام**:
- افتح rfid-guide.x.ai/simulator.
- اختر رقاقة (مثل MIFARE Classic).
- اقرأ UID، اكتب نص، اختبر التشفير.
- جرّب هجومًا (مثل التنصت على NTAG213).

- راجع لوحة المعلومات لتحليل النتائج. **مثال سيناريو**:
- اختر MIFARE Classic.
- اقرأ UID "04A1B2C3" من القطاع 0.
- حاول قراءة القطاع 1: "مطلوب مفتاح".
- أدخل مفتاح "FFFFFFFFFFFF": يُسمح بالقراءة.
- اكتب "Employee123" في القطاع 1.
- جرّب هجوم استخراج المفتاح: "نجح الهجوم، المفتاح ضعيف".
- اختر DESFire، حاول الهجوم: "فشل بسبب AES". **الصورة في الكتاب**:
- لقطة شاشة لواجهة الأداة تُظهر جدول MIFARE Classic وزر "محاكاة هجوم".
- تعليق: "مخطط 2.5: الأداة تُحاكي هيكلية الرقائق والهجمات الأمنية." **فوائد الأداة**:
- تبسيط هيكلية الرقائق.
- تعليم تأثير التشفير والهجمات.
- تمكين التجربة بدون أجهزة.

2.8 مخطط تدفق قراءة UID *(مخطط إضافي)*

الوصف: مخطط يوضح تدفق قراءة UID من رقاقة RFID باستخدام قارئ NFC (مثل هاتف). **الصورة في الكتاب**:

- رسم تدفقي:
  - **هاتف NFC**: يُرسل إشارة راديو (13.56 ميجاهرتز).
  - **رقاقة RFID**: ترد بـ UID (مثل "04A1B2C3").
  - **إذا كانت مشفرة**: القارئ يطلب مفتاحًا (مثل مفتاح A).
  - **النتيجة**: UID يظهر على التطبيق (مثل NFC Tools).
- ألوان: أزرق (إشارة راديو)، أحمر (UID)، أخضر (تطبيق).
- تعليق: "مخطط 2.6: تدفق قراءة UID يُظهر التفاعل بين القارئ والرقاقة."

```
+------------------------------------------+
|                    تدفق قراءة UID         |
+------------------------------------------+
| [هاتف NFC]                                |
| | NFC Tools                               |
| v                                         |
| ~~~ إشارة راديو (13.56 ميجاهرتز) ~~~      |
| |                                         |
| v                                         |
| [رقاقة RFID]                              |
| | UID: 04A1B2C3                           |
| | (إذا مشفرة: طلب مفتاح)                  |
| v                                         |
| ~~~ رد: UID ~~~                           |
| |                                         |
| v                                         |
| [هاتف NFC]                                |
| | عرض UID: 04A1B2C3                       |
+------------------------------------------+
```

- **شرح المخطط**:
  - يُظهر الإشارة من الهاتف إلى الرقاقة.
  - الرقاقة ترد بـ UID إذا لم تكن مشفرة.
  - إذا كانت مشفرة، يُطلب مفتاح.

2.9 إدارة المفاتيح في RFID *(قسم إضافي)*

الوصف: إدارة المفاتيح هي عملية تخزين، توزيع، وتحديث مفاتيح التشفير (مثل مفتاح A/B في MIFARE Classic أو AES في DESFire) لضمان أمان RFID.

- **لماذا إدارة المفاتيح؟**
  - تحمي البيانات من الوصول غير المصرح به.
  - تمنع هجمات مثل استخراج المفتاح أو التلاعب.
- **أنواع المفاتيح**:
  - **MIFARE Classic**: مفتاح A وB (48 بت) لكل قطاع.
  - **MIFARE DESFire**: مفاتيح AES/3DES لكل تطبيق.
  - **NTAG213**: كلمة مرور (32 بت، اختيارية).
- **عملية الإدارة**:
  - **التخزين**: حفظ المفاتيح في قاعدة بيانات مشفرة.
  - **التوزيع**: إرسال المفاتيح إلى القارئات بشكل آمن (مثل عبر HTTPS).
  - **التحديث**: تغيير المفاتيح دوريًا لتقليل مخاطر التسريب.
  - **النسخ الاحتياطي**: حفظ نسخة مشفرة للمفاتيح.

- **التحديات**:
  - فقدان المفتاح يمنع الوصول إلى البيانات.
  - المفاتيح الافتراضية (مثل "FFFFFFFFFFFF") تزيد المخاطر.
  - إدارة مفاتيح متعددة في أنظمة كبيرة معقدة.
- **الحلول**:
  - استخدام أنظمة إدارة مفاتيح (KMS) مثل AWS KMS.
  - تغيير المفاتيح الافتراضية عند التهيئة.
  - تدريب الموظفين على إدارة المفاتيح.
- **مثال عملي**:
  - نظام دخول مبنى:
    - كل بطاقة MIFARE Classic لها مفتاح A فريد.
    - المفاتيح تُخزن في خادم مشفر.
    - يتم تحديث المفاتيح كل 6 أشهر.

رسم توضيحي:

- صورة: خادم يُخزن مفاتيح AES، قارئ يطلب مفتاحًا، رقاقة DESFire تُصادق.
- تعليق: "مخطط 2.7: إدارة المفاتيح تُحمي بيانات RFID."

ملخص القسم

- هيكلية MIFARE Classic تُنظم البيانات في قطاعات/كتل، لكن تشفيرها ضعيف.
- NTAG213 تُستخدم لـ NDEF في صفحات، مع حماية محدودة.
- MIFARE DESFire تُنظم البيانات في تطبيقات/ملفات، مع تشفير قوي.
- التمرين يتيح قراءة UID، كتابة NDEF، واختبار التشفير.
- الأداة التفاعلية تُحاكي الهيكلية والهجمات.
- إدارة المفاتيح ضرورية للأمان.

أسئلة مراجعة

- كيف تختلف هيكلية MIFARE Classic عن MIFARE DESFire؟
- لماذا تُعتبر NTAG213 غير آمنة للدفع؟
- ماذا تعلمت من كتابة NDEF واختبار التشفير؟
- كيف تُساعد الأداة التفاعلية في فهم الهجمات؟
- لماذا تُعتبر إدارة المفاتيح تحديًا في RFID؟

موارد إضافية

- **فيديوهات**:
  - "هيكلية MIFARE Classic" (youtube.com/mifare-structure (#)).
  - "إدارة المفاتيح في RFID" (youtube.com/rfid-key-management (#)).
- **موقع**: rfid-guide.x.ai.

- **تطبيقات**: NFC Tools، NXP TagInfo.
- **أداة تفاعلية**: rfid-guide.x.ai/simulator.

2.3 هيكلية رقائق RFID *(ملخص القسم السابق مع الإضافات)*

هذا القسم يشرح هيكلية رقائق RFID (MIFARE Classic، NTAG213، MIFARE DESFire)، مع التركيز على تنظيم البيانات (UID، بيانات القطاعات، NDEF) والأمان. يُدمج مع الأداة التفاعلية الموسعة، مخطط كتابة NDEF، وقسم مقارنة RFID مع Bluetooth.

ملخص هيكلية الرقائق (من القسم السابق):

- **MIFARE Classic**:
  - ذاكرة: 1K/4K بايت، 16/40 قطاعًا، كل قطاع 4 كتل (16 بايت).
  - القطاع 0، الكتلة 0: UID وبيانات المصنع.
  - الكتلة 3: مفاتيح A/B وإعدادات الوصول.
  - تشفير: CRYPTO1 (ضعيف).
- **NTAG213**:
  - ذاكرة: 144 بايت قابلة للكتابة، 45 صفحة (4 بايت لكل صفحة).
  - الصفحة 0-2: UID وبيانات المصنع.
  - الصفحات 4-39: بيانات NDEF.
  - الأمان: بدون تشفير، قفل اختياري أو كلمة مرور.
- **MIFARE DESFire**:
  - ذاكرة: 2K/4K/8K بايت، تطبيقات (حتى 28) وملفات.
  - UID: محمي، ثابت أو عشوائي.
  - تشفير: AES/3DES (قوي).

مخططات سابقة:

- قدمت مخططات ASCII لهيكلية MIFARE Classic، NTAG213، وDESFire.
- قدمت مخطط ASCII لتدفق قراءة UID.

2.7 أداة تفاعلية: محاكاة هيكلية القطاعات مع إدارة المفاتيح *(موسعة)*

الوصف: أداة رقمية تفاعلية (متوفرة على rfid-guide.x.ai) تُحاكي هيكلية رقائق RFID (MIFARE Classic، NTAG213، DESFire)، مع ميزات جديدة لمحاكاة **إدارة المفاتيح** و**الهجمات الأمنية**. الأداة تُعزز فهم تنظيم البيانات، التشفير، وإدارة الأمان.

الهدف:

- تصور هيكلية الرقائق (قطاعات، صفحات، تطبيقات).
- محاكاة قراءة/كتابة البيانات.
- محاكاة هجمات أمنية (مثل التنصت، استخراج المفتاح).
- محاكاة إدارة المفاتيح (تخزين، تحديث، توزيع المفاتيح).

مكونات الأداة:

- **واجهة المستخدم**:
  - لوحة تحكم تُظهر:

- **MIFARE Classic**: جدول 16 قطاعًا، 4 كتل لكل قطاع.
- **NTAG213**: شريط 45 صفحة.
- **MIFARE DESFire**: شجرة تطبيقات وملفات.
- أزرار تفاعلية: "قراءة"، "كتابة"، "إعدادات التشفير"، "محاكاة هجوم"، **"إدارة المفاتيح"** (جديد).

- **محاكاة القراءة/الكتابة**:
  - اختر رقاقة (مثل MIFARE Classic).
  - انقر على القطاع 0، الكتلة 0 لقراءة UID (مثل "04A1B2C3").
  - اكتب نص (مثل "Test2025") أو URL في قطاع/صفحة.
  - إذا كان القطاع مشفرًا، تظهر رسالة "مطلوب مفتاح".
- **محاكاة التشفير**:
  - لـ MIFARE Classic: أدخل مفتاح A/B (مثل "FFFFFFFFFFFF").
  - لـ NTAG213: أدخل كلمة مرور (إن وجدت).
  - لـ DESFire: أدخل مفتاح AES وهمي.
  - تظهر رسائل: "مصادقة ناجحة" أو "فشل المصادقة".
- **محاكاة هجمات أمنية** (من القسم السابق):
  - **التنصت**: اعتراض بيانات NTAG213 (مثل URL).
  - **استنساخ**: نسخ UID وبيانات MIFARE Classic.
  - **استخراج المفتاح**: كسر مفتاح CRYPTO1 في MIFARE Classic.
  - **حماية DESFire**: فشل الهجوم بسبب AES.
- **محاكاة إدارة المفاتيح** (*ميزة جديدة*):
  - **تخزين المفاتيح**:
    - أنشئ قاعدة بيانات وهمية لتخزين مفاتيح (مثل مفتاح A لكل قطاع في MIFARE Classic).
    - مثال: أدخل مفتاح A "A1B2C3D4E5F6" للقطاع 1.
    - الأداة تُظهر: "تم تخزين المفتاح في قاعدة بيانات مشفرة."
  - **توزيع المفاتيح**:
    - محاكاة إرسال مفتاح إلى قارئ RFID.
    - مثال: انقر "توزيع"، تظهر رسالة: "تم إرسال مفتاح A إلى القارئ عبر قناة آمنة."
  - **تحديث المفاتيح**:
    - غيّر مفتاحًا (مثل تغيير مفتاح A إلى "1234567890AB").
    - الأداة تُظهر: "تم تحديث مفتاح القطاع 1، الوصول مقتصر على المفتاح الجديد."
  - **نسخ احتياطي**:
    - احفظ نسخة مشفرة من المفاتيح.
    - مثال: انقر "نسخ احتياطي"، تظهر: "تم حفظ المفاتيح في ملف مشفر."
  - **محاكاة أخطاء**:
    - إذا أدخلت مفتاحًا خاطئًا: "فشل الوصول، مفتاح غير صحيح."
    - إذا فقد المفتاح: "لا يمكن الوصول إلى القطاع، أعد تعيين المفتاح."
- **لوحة المعلومات**:
  - تُظهر: UID، نوع الرقاقة، حجم الذاكرة، حالة التشفير.
  - رسم بياني: نسبة القطاعات المستخدمة.
  - سجل العمليات: (مثل "تم تحديث مفتاح القطاع 1"، "هجوم تنصت نجح على NTAG213").
  - **سجل إدارة المفاتيح** (جديد): يُظهر تخزين، توزيع، وتحديث المفاتيح.

كيفية الاستخدام:

- افتح rfid-guide.x.ai/simulator.
- اختر رقاقة (مثل MIFARE Classic).
- اقرأ UID، اكتب نص، اختبر التشفير.
- جرّب هجومًا (مثل استخراج مفتاح).
- انتقل إلى "إدارة المفاتيح":
  - أنشئ مفتاح A للقطاع 1.
  - وزّعه إلى قارئ وهمي.
  - غيّر المفتاح واختبر الوصول.
- راجع لوحة المعلومات لتحليل النتائج.

مثال سيناريو:

- اختر MIFARE Classic.
- اقرأ UID "04A1B2C3" من القطاع 0.
- حاول قراءة القطاع 1: "مطلوب مفتاح."
- في "إدارة المفاتيح":
  - أنشئ مفتاح A "A1B2C3D4E5F6" للقطاع 1.
  - وزّعه: "تم إرسال المفتاح إلى القارئ."
  - اكتب "Employee123" في القطاع 1: "نجحت الكتابة."
  - غيّر المفتاح إلى "1234567890AB": "تم التحديث."
  - حاول القراءة بالمفتاح القديم: "فشل المصادقة."
- جرّب هجوم استخراج المفتاح: "نجح بسبب ضعف CRYPTO1."
- اختر DESFire، حاول الهجوم: "فشل بسبب AES."

الصورة في الكتاب:

- لقطة شاشة لواجهة الأداة تُظهر جدول MIFARE Classic، زر "إدارة المفاتيح"، وسجل العمليات.
- تعليق: "مخطط 2.5: الأداة تُحاكي هيكلية الرقائق، الهجمات، وإدارة المفاتيح."

فوائد الأداة:

- تبسيط فهم هيكلية الرقائق والتشفير.
- تعليم إدارة المفاتيح عمليًا.
- محاكاة الهجمات تُظهر أهمية الأمان.
- مناسبة للتعلم دون أجهزة حقيقية.

تحدي إضافي:

- جرّب تحديث مفاتيح متعددة لقطاعات مختلفة في MIFARE Classic.
- قارن إدارة المفاتيح في MIFARE Classic (CRYPTO1) مع DESFire (AES) في الأداة.

2.8 مخطط تدفق كتابة بيانات NDEF *(مخطط إضافي)*

الوصف: مخطط يوضح تدفق كتابة بيانات NDEF (مثل نص أو URL) على رقاقة RFID (مثل NTAG213) باستخدام قارئ NFC (مثل هاتف).

الصورة في الكتاب:

- رسم تدفقي:
  - **هاتف NFC**: يفتح تطبيق NFC Tools، يختار "Text Record" → "Write".
  - **إدخال البيانات**: المستخدم يكتب نصًا (مثل "MyRFIDTest2025") أو URL.
  - **إشارة راديو**: الهاتف يُرسل إشارة (13.56 ميجاهرتز) إلى الرقاقة.
  - **رقاقة RFID**: تتحقق من إعدادات القفل أو كلمة المرور (إن وجدت).
  - **كتابة البيانات**: النص يُخزن في الصفحات (مثل 4-10 في NTAG213) بتنسيق NDEF.
  - **النتيجة**: رسالة نجاح على التطبيق.
- ألوان: أزرق (إشارة راديو)، أخضر (بيانات NDEF)، أحمر (تطبيق).
- تعليق: "مخطط 2.6: تدفق كتابة NDEF يُظهر التفاعل بين القارئ والرقاقة."

تصميم ASCII لتدفق كتابة NDEF:

```
+------------------------------------------+
|           تدفق كتابة بيانات NDEF           |
+------------------------------------------+
| [هاتف NFC]                               |
| | NFC Tools: اختر "Write"                 |
| | أدخل نص: MyRFIDTest2025                  |
| v                                        |
| ~~~ إشارة راديو (13.56 ميجاهرتز) ~~~       |
| |                                        |
| v                                        |
| [رقاقة RFID: NTAG213]                     |
| | تحقق: هل مقفلة؟ (لا)                    |
| | (إذا محمية: طلب كلمة مرور)               |
| v                                        |
| ~~~ كتابة: نص NDEF ~~~                    |
| | [صفحات 4-10: MyRFIDTest2025]             |
| v                                        |
| [هاتف NFC]                               |
| | عرض: "تمت الكتابة بنجاح"                 |
+------------------------------------------+
```

شرح المخطط:

يُظهر إدخال النص في التطبيق.

الرقاقة تتحقق من إعدادات القفل.

النص يُخزن بتنسيق NDEF إذا سمحت الرقاقة.

الدمج في الكتاب:

الصورة تُضاف تحت عنوان "مخطط 2.6".

تعليق: "يوضح المخطط كيفية كتابة بيانات NDEF على NTAG213."

2.10 مقارنة RFID مع Bluetooth (قسم إضافي)

الوصف: هذا القسم يقارن تقنيتي RFID وBluetooth من حيث الآلية، التطبيقات، الأمان، والأداء، لتوضيح متى تُستخدم كل تقنية.

1. الآلية:

RFID:

تستخدم موجات راديو لنقل البيانات (LF: 125-134 كيلوهرتز، HF: 13.56 ميجاهرتز، UHF: 860-960 ميجاهرتز).

الاتصال: أحادي أو ثنائي محدود (في NFC).

لا يتطلب طاقة في الرقائق السلبية (تعمل بطاقة القارئ).

Bluetooth:

تستخدم موجات راديو (2.4 جيجاهرتز).

الاتصال: ثنائي، يدعم نقل البيانات المستمر.

يتطلب طاقة في كلا الجهازين (مثل الهاتف والسماعة).

2. النطاق:

RFID:

LF/HF: حتى 1 متر (NFC: 10 سم).

UHF: حتى 15 مترًا.

Bluetooth:

Bluetooth Low Energy (BLE): حتى 100 متر.

Bluetooth Classic: حتى 10 أمتار.

3. سعة البيانات:

RFID:

صغيرة (بايتات إلى كيلوبايتات).

مثال: NTAG213 (144 بايت)، MIFARE DESFire (8K بايت).

Bluetooth:

كبيرة (ميجابايتات إلى جيجابايت).

مثال: نقل ملفات صوتية أو فيديو.

4. الأمان:

RFID:

يعتمد على الرقاقة:

MIFARE Classic: CRYPTO1 (ضعيف).

MIFARE DESFire: AES/3DES (قوي).

NTAG213: بدون تشفير افتراضي.

عرضة للتنصت (خاصة UHF) أو الاستنساخ (MIFARE Classic).

:Bluetooth
تشفير AES-128 (في BLE) أو E0 (في Classic).

مصادقة الاقتران (Pairing) تحمي الاتصال.

أقل عرضة للتنصت بسبب الاقتران والنطاق القصير.

5. التطبيقات:
:RFID
تتبع المخزون (مستودعات، متاجر مثل Zara).

التحكم بالوصول (بطاقات المكاتب).

الدفع بدون تلامس (NFC).

النقل العام (بطاقات مترو).

:Bluetooth
الأجهزة القابلة للارتداء (ساعات ذكية).

نقل الصوت (سماعات لاسلكية).

إنترنت الأشياء (مثل أجهزة المنزل الذكي).

تحديد المواقع (BLE Beacons).

6. التكلفة:
:RFID
الرقائق رخيصة (NTAG213: ~0.2 دولار، DESFire: ~1 دولار).

القارئات تتراوح من رخيصة (هواتف NFC) إلى مكلفة (قارئات UHF).

:Bluetooth
الأجهزة أغلى بسبب الحاجة إلى طاقة ومعالجات.

مثال: وحدة BLE تكلف ~5 دولارات.

7. التوافق:
:RFID

محدود بالتردد (LF، HF، UHF) ونوع الرقاقة.

NFC متوافق مع معظم الهواتف الذكية.

Bluetooth:
متوافق عالميًا (BLE مدعوم في معظم الأجهزة).

يتطلب إصدارات متطابقة (مثل Bluetooth 5.0).

جدول مقارنة:
الخاصية

RFID

Bluetooth

الآلية

موجات
راديو
(LF،
HF،
UHF)

موجات
راديو
(2.4
جيجاهرتز)

النطاق

حتى
15
مترًا
(UHF)،
10
سم
(NFC)

حتى
100
متر
(BLE)

سعة
البيانات

بايتات
إلى
كيلوبايتات

ميجابايتات
إلى
جيجابايت

الأمان

CRYPTO1/AES
(يعتمد
على
الرقاقة)

AES-128،
اقتران

التطبيقات

تتبع،
دخول،
دفع،
نقل

صوت،
IoT،
مواقع

التكلفة

رخيصة
(رقائق)،
قارئات
متنوعة

أغلى
(أجهزة
نشطة)

التوافق

محدود
بالتردد

عالمي
BLE)
شائع)

مثال عملي:
RFID: ملصق NTAG213 في متجر يُخزن رابط URL للمنتج، يُقرأ بهاتف NFC في ثوانٍ.

Bluetooth: منارة BLE في متجر ترسل إشعارات إلى الهواتف ضمن نطاق 50 مترًا، لكنها تتطلب تطبيقًا واتصالًا نشطًا.

متى تُستخدم كل تقنية؟:
RFID: للتطبيقات السلبية، منخفضة التكلفة، مثل تتبع المخزون أو الدفع السريع.

Bluetooth: للتطبيقات التفاعلية، عالية البيانات، مثل الأجهزة القابلة للارتداء أو المنازل الذكية.

رسم توضيحي:
صورة مقسمة:
RFID: هاتف يقرأ ملصق NFC، مع رمز NDEF.

Bluetooth: هاتف يتصل بسماعة لاسلكية، مع رمز اقتران.

تعليق: "مخطط 2.7: RFID مناسب للتتبع السريع، Bluetooth للاتصال التفاعلي."

أسئلة للتفكير:
لماذا تُعتبر RFID أكثر ملاءمة لتتبع المخزون من Bluetooth؟

كيف يؤثر التشفير على اختيار RFID مقابل Bluetooth في الدفع؟

ملخص الفصل (مع الإضافات)
هيكلية رقائق RFID (MIFARE Classic، NTAG213، DESFire) تُحدد تنظيم البيانات والأمان.

الأداة التفاعلية تُحاكي الهيكلية، الهجمات، وإدارة المفاتيح، مما يسهل التعلم.

مخطط كتابة NDEF يوضح التفاعل بين القارئ والرقاقة.

مقارنة RFID مع Bluetooth تُظهر اختلافات النطاق، البيانات، والتطبيقات.

أسئلة مراجعة
كيف تُساعد محاكاة إدارة المفاتيح في الأداة التفاعلية على فهم الأمان؟

ماذا يُظهر مخطط كتابة NDEF عن عملية تخزين البيانات؟

لماذا تُستخدم RFID بدلًا من Bluetooth في تتبع المخزون؟

كيف تختلف إدارة المفاتيح في MIFARE Classic عن DESFire؟

ما الفرق بين هيكلية NTAG213 وMIFARE DESFire؟

موارد إضافية
فيديوهات:
"إدارة المفاتيح في RFID" (youtube.com/rfid-key-management (#)).

"RFID مقابل Bluetooth" (youtube.com/rfid-vs-bluetooth (#)).

موقع: rfid-guide.x.ai.

تطبيقات: NFC Tools، NXP TagInfo.

أداة تفاعلية: rfid-guide.x.ai/simulator.

الفصل الثالث: الأدوات

أهداف الفصل

- فهم الأدوات الأساسية للعمل مع RFID (قارئات، برامج، رقائق).
- استكشاف واجهة NFC Tools عمليًا من خلال تمرين.
- مقارنة قارئي RFID (ACR122U وPN532) من حيث السعر، الميزات، والأداء.
- تقديم إرشادات لاختيار الأدوات بناءً على التطبيقات (مثل الدخول، التتبع، الدفع).
- محاكاة سيناريوهات عملية باستخدام الأدوات.

3.1 مقدمة عن أدوات RFID

أدوات RFID تشمل الأجهزة (مثل القارئات) والبرامج (مثل NFC Tools) والرقائق (مثل MIFARE Classic). هذا الفصل يركز على كيفية استخدام هذه الأدوات لقراءة وكتابة البيانات، مع شرح عملي للبرامج والأجهزة الشائعة. الهدف هو تمكين القارئ من اختيار الأدوات المناسبة بناءً على احتياجاته.

3.1.1 أنواع الأدوات

- **القارئات**:
  - **ACR122U**: قارئ USB للكمبيوتر، يدعم NFC، MIFARE، وISO 14443 A/B.
  - **PN532**: وحدة NFC متعددة الواجهات (UART، I2C، SPI)، مناسبة لمشاريع Arduino.
  - أمثلة أخرى: Proxmark3 (متقدم)، قارئات الهواتف الذكية (NFC مدمج).
- **البرامج**:
  - **NFC Tools**: تطبيق للهواتف الذكية لقراءة/كتابة NFC.
  - **MTools**: لتعديل MIFARE Classic وUltralight.
  - **NXP TagInfo**: لتحليل نوع الرقاقة والتشفير.

- **الرقائق**:
  - MIFARE Classic (1K/4K): شائعة في الدخول والنقل.
  - NTAG213/215/216: لملصقات NFC.
  - MIFARE DESFire: للدفع والتطبيقات الآمنة.

3.1.2 أهمية الأدوات

- **القراءة**: استخراج UID وبيانات القطاعات.
- **الكتابة**: تعديل البيانات (مثل أرقام، أسماء، روابط).
- **الأمان**: اختبار التشفير وإدارة المفاتيح.
- **التطبيقات**: تتبع المخزون، التحكم بالوصول، الدفع بدون تلامس.

3.2 استكشاف NFC Tools

الوصف: NFC Tools هو تطبيق مجاني (مع ميزات مدفوعة) لنظامي Android وiOS، يُستخدم لقراءة وكتابة رقائق NFC/RFID باستخدام هاتف ذكي يدعم NFC. التطبيق سهل الاستخدام ويدعم رقائق مثل MIFARE Classic، NTAG213، وUltralight.

الميزات:

- **القراءة**: عرض UID، نوع الرقاقة، حجم الذاكرة، البيانات (مثل NDEF).
- **الكتابة**: إضافة نصوص، روابط URL، بيانات مخصصة.
- **المهام**: إنشاء إجراءات (مثل فتح تطبيق عند قراءة الرقاقة).
- **التوافق**: يعمل مع معظم رقائق NFC (ISO 14443 A/B).

متطلبات التشغيل:

- هاتف ذكي يدعم NFC (مثل iPhone 7، Samsung Galaxy أو أحدث).
- نظام تشغيل: Android 5.0+ أو iOS 13+.
- تطبيق NFC Tools (متوفر على Google Play/App Store).

تمرين: تنزيل NFC Tools واستكشاف واجهة المستخدم

الهدف: تثبيت NFC Tools، استكشاف واجهة "Write"، والتقاط لقطة شاشة.

الأدوات المطلوبة:

- هاتف ذكي يدعم NFC.
- اتصال إنترنت لتحميل التطبيق.
- دفتر ملاحظات أو تطبيق تدوين.

الخطوات:

- **تنزيل NFC Tools**:
  - افتح Google Play (Android) أو App Store (iOS).
  - ابحث عن "NFC Tools" (المطور: wakdev).
  - انقر "تثبيت" (حجم التطبيق حوالي 9 ميجابايت).
  - انتظر حتى اكتمال التثبيت (يستغرق 1-2 دقيقة حسب الاتصال).
- **فتح التطبيق**:

- شغّل NFC Tools من قائمة التطبيقات.
- فعّل NFC في إعدادات الهاتف (إعدادات → اتصالات → NFC).
- امنح الأذونات المطلوبة (مثل الوصول إلى الموقع لنظام Android).
- **استكشاف واجهة "Write"**:
  - في الشاشة الرئيسية، سترى خيارات: Read، Write، Other، Tasks.
  - انقر على "Write".
  - ستظهر واجهة تحتوي على:
    - **Add a Record**: خيارات مثل Text، URL، Contact، Email.
    - **Current Records**: قائمة السجلات المُعدة للكتابة.
    - **Write Button**: زر لتأكيد الكتابة على الرقاقة.
    - **Options**: إعدادات متقدمة (مثل الحماية بكلمة مرور).
  - جرب إضافة سجل:
    - انقر "Add a Record" → "Text".
    - اكتب نصًا (مثل "Test2025").
    - انقر "OK" لإضافته إلى قائمة السجلات.
- **التقاط لقطة شاشة**:
  - تأكد من أن واجهة "Write" مفتوحة (مع السجل "Test2025" مرئي).
  - التقط لقطة شاشة:
    - Android: اضغط زر الطاقة + خفض الصوت.
    - iOS: اضغط زر الطاقة + زر الشاشة الرئيسية (أو زر رفع الصوت في الإصدارات الحديثة).
  - احفظ اللقطة في معرض الصور.
- **تسجيل الملاحظات**:
  - دوّن:
    - هل كان التثبيت سهلاً؟ (مثل "التثبيت استغرق دقيقة").
    - وصف واجهة "Write" (مثل "تحتوي على زر Add a Record وخيارات Text/URL").
    - أي مشكلات (مثل "NFC لم يُفعّل تلقائيًا").
  - أرفق لقطة الشاشة (يمكنك رفعها إلى rfid-guide.x.ai).
- **تحليل الواجهة**:
  - اكتب فقرة (100-150 كلمة) تصف تجربتك:
    - سهولة التنقل في الواجهة.
    - وضوح الخيارات (مثل Text، URL).
    - ما تعلمته (مثل كيفية إضافة سجل).
  - مثال: "قمت بتثبيت NFC Tools بسهولة من Google Play في دقيقة. واجهة 'Write' واضحة، تحتوي على زر 'Add a Record' لإضافة نصوص أو روابط. أضفت نص 'Test2025' بسهولة، لكن لاحظت أن التطبيق يتطلب تفعيل NFC يدويًا. الواجهة سهلة الاستخدام للمبتدئين، لكن خيارات الحماية المتقدمة تحتاج إلى خبرة. تعلمت أن NFC Tools يُبسط كتابة البيانات، لكنه قد يحتاج إلى رقاقة غير مقفلة للكتابة."

معايير النجاح:

- تثبيت NFC Tools بنجاح.
- الوصول إلى واجهة "Write".
- التقاط لقطة شاشة واضحة.
- كتابة فقرة تحليلية مع ملاحظات.

صورة توضيحية:

- لقطة شاشة لواجهة "Write" تُظهر السجل "Test2025".
- تعليق: "مخطط 3.1: واجهة Write في NFC Tools تُظهر خيارات إضافة السجلات."

تحدي إضافي:

- جرب إضافة سجل URL (مثل "https://x.ai") ودوّن الخطوات.
- استكشف خيار "Protect Tag" في الإعدادات المتقدمة.

3.3 مقارنة قارئي RFID: ACR122U وPN532

الوصف: قارئا ACR122U وPN532 هما من أشهر أجهزة RFID/NFC، يُستخدمان في قراءة وكتابة الرقائق. هذا القسم يقارن بينهما من حيث **السعر**، **الميزات**، **التوافق**، و**التطبيقات** بناءً على البيانات المتاحة.

تمرين: مقارنة بين ACR122U وPN532 من حيث السعر والميزات

الهدف: جمع بيانات عن السعر والميزات، إنشاء جدول مقارنة، وكتابة تحليل.

الأدوات المطلوبة:

- جهاز كمبيوتر أو هاتف ذكي مع اتصال إنترنت.
- دفتر ملاحظات أو برنامج (مثل Microsoft Word).
- مواقع موثوقة (Amazon، Adafruit، MTools Tec).

الخطوات:

- **البحث عن السعر**:
  - زر مواقع مثل Amazon، Adafruit، أو MTools Tec.
  - سجّل السعر الحالي (بما في ذلك تكاليف الشحن إن أمكن):
    - **ACR122U**: حوالي 25-30 دولارًا (متوسط السوق في 2025).
    - **PN532**: حوالي 10-15 دولارًا (وحدة بدون Bluetooth، أو 20-30 دولارًا مع BLE).
  - دوّن مصدر السعر (مثل رابط Amazon).
- **جمع الميزات**:
  - راجع مواصفات كل قارئ من مواقع الشركات المصنعة أو الموزعين.
  - ركز على:
    - التردد (مثل 13.56 ميجاهرتز).
    - الرقائق المدعومة (MIFARE، NTAG، DESFire).
    - الواجهات (USB، UART، I2C، SPI).
    - المسافة (مدى القراءة).
    - التوافق (Windows، Linux، Arduino).
    - ميزات إضافية (مثل LED، صوت تنبيه).
- **إنشاء جدول مقارنة**:
  - استخدم الجدول التالي كقالب:

ا	ACR122U	PN532
ا	25-30 دولارًا	10-15 دولارًا (20-30 مع BLE)
ا	13.56 ميجاهرتز	13.56 ميجاهرتز
ا	MIFARE Classic، Ultralight، DESFire، NTAG، FeliCa	MIFARE Classic، Ultralight، DESFire، NTAG، FeliCa

ا	(USB (PC/SC، CCID	UART، I2C، SPI، (BLE اختياري)
م	حتى 5 سم	حتى 5 سم
ا	Windows، Mac، Linux	Arduino، Raspberry Pi، PC (مع وحدات)

م	LED (أحمر/أخضر)، صوت تنبيه، SDK	مفتاح DIP لتغيير الواجهة، وضع توفير الطاقة
ا	الدفع، الدخول، تطوير البرمجيات	مشاريع IoT، DIY، اختبار الأمان

- ملاحظات:
  - **ACR122U**: قارئ USB جاهز، سهل التثبيت على أجهزة الكمبيوتر، يدعم PC/SC وCCID، مناسب للتطبيقات التجارية.
  - **PN532**: وحدة مرنة، تدعم واجهات متعددة (UART، I2C، SPI)، مثالية لمشاريع Arduino وRaspberry Pi، لكنها تتطلب تهيئة.
- **تحليل المقارنة**:
  - اكتب فقرة (150-200 كلمة) تجيب على:
    - أي قارئ أفضل للمبتدئين؟ للمحترفين؟
    - كيف يؤثر السعر على الاختيار؟
    - ما التطبيقات الأنسب لكل قارئ؟
  - مثال: "ACR122U بسعر 25-30 دولارًا هو قارئ USB سهل الاستخدام، مثالي للمبتدئين بفضل توافقه مع Windows/Linux وتثبيته البسيط (PC/SC). يدعم MIFARE Classic، DESFire، وNTAG، مما يجعله مناسبًا للدفع والدخول. PN532، بسعر 10-15 دولارًا (أو 20-30 مع BLE)، أرخص ومرن بفضل واجهاته (UART، I2C، SPI)، لكنه يتطلب خبرة في البرمجة (مثل Arduino)، مما يجعله مفضلًا

للمحترفين في مشاريع IoT. السعر يجعل PN532 جذابًا للميزانيات المنخفضة، بينما ACR122U يوفر راحة أكبر. ACR122U أفضل للتطبيقات التجارية، وPN532 للتطوير التجريبي."

- **تسجيل النتائج**:
  - أرفق الجدول والفقرة في تقرير.
  - أضف لقطات شاشة لصفحات الأسعار (مثل Amazon).
  - ارفع التقرير إلى rfid-guide.x.ai (اختياري).

معايير النجاح:

- جمع بيانات دقيقة للسعر والميزات.
- إنشاء جدول مقارنة واضح.
- كتابة فقرة تحليلية.
- توثيق المصادر (مثل روابط المواقع).

صورة توضيحية:

- صورة مقسمة: ACR122U (قارئ USB أبيض) وPN532 (وحدة حمراء مع DIP).
- تعليق: "مخطط 3.2: ACR122U وPN532 يدعمان NFC، لكن بتصميمات واستخدامات مختلفة."

تحدي إضافي:

- ابحث عن قارئ ثالث (مثل Proxmark3) وقارنه مع ACR122U وPN532.
- تحقق من توافر برامج تشغيل (Drivers) لكل قارئ على Windows/Linux.

3.4 إرشادات اختيار الأدوات

- **للمبتدئين**:
  - اختر هاتفًا ذكيًا مع NFC وNFC Tools لسهولة الاستخدام.
  - ACR122U للكمبيوتر (تثبيت بسيط).
- **للمحترفين**:
  - PN532 لمشاريع DIY (Arduino، Raspberry Pi).
  - Proxmark3 لاختبار الأمان والهجمات.
- **حسب التطبيق**:
  - الدفع/الدخول: MIFARE DESFire، ACR122U.
  - التتبع/الملصقات: NTAG213، NFC Tools.
  - التطوير: MTools، PN532.

مخطط ASCII لعملية اختيار الأدوات:

```
+------------------------------------------+
|        عملية اختيار أدوات RFID          |
+------------------------------------------+
| [حدد التطبيق]                            |
| | (مثل الدفع، التتبع، الدخول)            |
| v                                        |
| [حدد الميزانية]                          |
| | (مثل 10 دولارات، 30 دولارًا)           |
| v                                        |
| [اختر القارئ]                            |
| | ACR122U: سهل، USB                      |
| | PN532: مرن، DIY                        |
| v                                        |
| [اختر البرنامج]                          |
| | NFC Tools: للمبتدئين                   |
| | MTools: للمحترفين                      |
| v                                        |
| [اختيار الأداة]                          |
| | (مثل قراءة UID، كتابة NDEF)            |

+------------------------------------------+
```

- **شرح المخطط:**
  - يوضح خطوات اختيار القارئ والبرنامج بناءً على التطبيق والميزانية.
- **الصورة في الكتاب:**
  - رسم تدفقي ملون يُظهر القرارات (مثل التطبيق ← الميزانية ← القارئ).
  - تعليق: "مخطط 3.3: عملية اختيار الأدوات تُبسط اختيار القارئ والبرنامج."

ملخص الفصل

- الأدوات (قارئات، برامج، رقائق) ضرورية لقراءة وكتابة RFID.
- NFC Tools تطبيق سهل للمبتدئين، مع واجهة "Write" واضحة.
- ACR122U مناسب للتطبيقات التجارية، بينما PN532 مثالي للتطوير.
- اختيار الأدوات يعتمد على التطبيق، الميزانية، ومستوى الخبرة.

أسئلة مراجعة

- ما الفرق بين ACR122U وPN532 من حيث الواجهات؟
- كيف تُساعد واجهة "Write" في NFC Tools على كتابة البيانات؟
- ما العوامل التي تؤثر على اختيار قارئ RFID؟
- لماذا يُفضل PN532 في مشاريع DIY؟
- كيف يمكن تحسين تجربة استخدام NFC Tools؟

موارد إضافية

- **فيديوهات**:
  - "تثبيت NFC Tools" (youtube.com/nfc-tools-install (#)).
  - "مقارنة ACR122U وPN532" (youtube.com/acr122u-vs-pn532 (#)).
- **موقع**: rfid-guide.x.ai.
- **تطبيقات**: NFC Tools، MTools، NXP TagInfo.
- **وثائق**:
  - دليل ACR122U: www.acs.com.hk.
  - دليل PN532: www.nxp.com.

الفصل الخامس: خطوات التغيير

أهداف الفصل

- تعلم كيفية تغيير بيانات رقائق RFID (مثل أرقام، نصوص).
- استخدام NFC Tools لكتابة بيانات جديدة على MIFARE Classic.
- تجربة تغيير بيانات في قطاع غير محمي وتسجيل النتائج.
- فهم قيود التشفير والحماية في الرقائق.
- تقديم إرشادات لضمان الأمان عند التغيير.

5.1 مقدمة عن تغيير بيانات RFID

تغيير بيانات RFID يعني تعديل البيانات المخزنة (مثل UID، أرقام، نصوص) في قطاعات/صفحات الرقاقة. هذا يتطلب:

- قارئ متوافق (مثل هاتف NFC أو ACR122U).
- برنامج (مثل NFC Tools أو MTools).
- رقاقة قابلة للكتابة (غير مقفلة أو بمفتاح معروف). العملية حساسة، خاصة مع الرقائق المحمية (مثل MIFARE Classic بمفتاح A/B).

5.1.1 قيود التغيير

- **الرقائق المحمية**: تتطلب مفتاحًا (مثل "FFFFFFFFFFFF" في MIFARE Classic).
- **القفل الدائم**: بعض الرقائق (مثل NTAG213) تصبح للقراءة فقط بعد القفل.
- **أخطاء الكتابة**: قد تُفسد البيانات إذا كان التنسيق غير صحيح.
- **الأمان**: تغيير UID قد يكون غير قانوني في بعض التطبيقات (مثل الدفع).

5.1.2 الأدوات المطلوبة

- هاتف ذكي يدعم NFC مع NFC Tools.
- رقاقة MIFARE Classic 1K/4K (يفضل "Magic Card" قابلة للتعديل).
- مفتاح افتراضي (مثل "FFFFFFFFFFFF") أو مفتاح معروف.
- دفتر ملاحظات لتسجيل النتائج.

5.2 تمرين: كتابة رقم جديد على MIFARE Classic باستخدام NFC Tools

الهدف: استخدام NFC Tools لكتابة رقم جديد (مثل "1234") على رقاقة MIFARE Classic، ثم قراءة الرقاقة للتحقق.
الأدوات المطلوبة:

- هاتف ذكي يدعم NFC مع NFC Tools مثبت.
- رقاقة MIFARE Classic 1K/4K (يفضل Gen1 أو CUID قابلة للكتابة بدون مفتاح).
- مفتاح افتراضي (مثل "FFFFFFFFFFFF") إذا كانت الرقاقة محمية.
- تطبيق MTools (اختياري للتعامل مع المفاتيح).

الخطوات:

- **إعداد الأدوات:**
  - تأكد من تثبيت NFC Tools (راجع تمرين الفصل الثالث).
  - فعّل NFC في إعدادات الهاتف.
  - جهّز رقاقة MIFARE Classic (تأكد أنها ليست بطاقة حساسة مثل بطاقة دفع).
- **اختبار الرقاقة:**
  - افتح NFC Tools، انقر "Read".
  - ضع الرقاقة خلف الهاتف.
  - سجّل:
    - UID (مثل "04A1B2C3").
    - نوع الرقاقة (MIFARE Classic 1K/4K).
    - حالة القطاعات (هل هي محمية؟).
  - إذا ظهرت رسالة "مطلوب مفتاح"، استخدم MTools لإدخال مفتاح افتراضي:
    - افتح MTools، انقر "Sector 0" ← "Read".
    - أدخل مفتاح A: "FFFFFFFFFFFF".
    - إذا نجحت المصادقة، تابع.
- **كتابة الرقم الجديد:**
  - في NFC Tools، انقر "Write".
  - انقر "Add a Record" ← "Text".
  - أدخل الرقم "1234".
  - انقر "OK" لإضافته إلى قائمة السجلات.
  - ضع الرقاقة خلف الهاتف، انقر "Write".
  - انتظر رسالة "Write Successful" (تستغرق 2-3 ثوانٍ).
  - إذا فشلت الكتابة (مثل "Tag is Locked")، تحقق من:
    - هل القطاع محمي؟ (استخدم MTools لإدخال المفتاح).
    - هل الرقاقة مقفلة نهائيًا؟ (غير قابلة للكتابة).
- **التحقق من الكتابة:**
  - انقر "Read" في NFC Tools.
  - ضع الرقاقة خلف الهاتف.
  - تحقق من ظهور "1234" في البيانات (عادةً في القطاع 1، الكتلة 0).
  - التقط لقطة شاشة للنتيجة.
- **تسجيل النتائج:**
  - دوّن:
    - UID.
    - نوع الرقاقة.
    - نتيجة الكتابة (مثل "كتبت 1234 بنجاح في القطاع 1").
    - أي مشكلات (مثل "فشلت الكتابة بسبب المفتاح").

- أرفق لقطة الشاشة.
- **تحليل النتائج**:
  - اكتب فقرة (150-200 كلمة):
    - وصف العملية.
    - هل نجحت الكتابة؟ لماذا؟
    - ما تعلمته (مثل أهمية المفتاح أو قيود NFC Tools).
  - مثال: "استخدمت NFC Tools لكتابة الرقم '1234' على رقاقة MIFARE Classic 1K. قرأت الرقاقة أولًا للتأكد من أن القطاع 1 غير محمي، ولم أحتج إلى مفتاح. الكتابة نجحت في ثوانٍ، وأكدت القراءة ظهور '1234' في الكتلة 0 من القطاع 1. واجهت مشكلة في البداية بسبب وضع الرقاقة بشكل غير صحيح خلف الهاتف. تعلمت أن NFC Tools يُبسط الكتابة للرقائق غير المحمية، لكن الرقائق المشفرة تحتاج إلى أدوات مثل MTools لإدارة المفاتيح. العملية أوضحت أهمية التحقق من حالة الرقاقة قبل الكتابة."

معايير النجاح:

- كتابة "1234" بنجاح (أو محاولة إذا كانت الرقاقة محمية).
- التحقق من البيانات بالقراءة.
- تسجيل النتائج مع لقطة شاشة.
- كتابة فقرة تحليلية.

صورة توضيحية:

- لقطة شاشة: نتيجة القراءة تُظهر "1234" في NFC Tools.
- تعليق: "مخطط 5.1: كتابة رقم جديد على MIFARE Classic باستخدام NFC Tools."

تحدي إضافي:

- جرب كتابة نص آخر (مثل "Test2025") في قطاع مختلف.
- إذا كانت الرقاقة محمية، استخدم MTools لإدخال مفتاح وكرر التمرين.

5.3 تمرين: تغيير بيانات في قطاع غير محمي

الهدف: تغيير بيانات في قطاع غير محمي في MIFARE Classic (مثل كتابة اسم "Ali")، وتسجيل النتائج (نجاح/فشل).
الأدوات المطلوبة:

- هاتف ذكي يدعم NFC مع NFC Tools.
- رقاقة MIFARE Classic 1K/4K (يفضل Gen1/CUID غير محمية).
- تطبيق MTools (اختياري لتحديد القطاعات غير المحمية).
- دفتر ملاحظات.

الخطوات:

- **تحديد قطاع غير محمي**:
  - افتح NFC Tools، انقر "Read".
  - ضع الرقاقة خلف الهاتف.
  - تحقق من القطاعات (مثل القطاع 1-15 في MIFARE Classic 1K).
  - إذا ظهرت رسالة "مطلوب مفتاح" لقطاع معين، فهو محمي.
  - استخدم MTools (اختياري):

- انقر "Scan Sectors" → "Read".
- أدخل مفتاح افتراضي "FFFFFFFFFFFF" لكل قطاع.
- سجّل القطاعات غير المحمية (مثل "القطاع 2: يمكن الكتابة").
  - اختر قطاعًا غير محمي (مثل القطاع 2).
- **كتابة البيانات**:
  - في NFC Tools، انقر "Write".
  - انقر "Add a Record" → "Text".
  - أدخل نصًا (مثل "Ali").
  - انقر "OK".
  - ضع الرقاقة خلف الهاتف، انقر "Write".
  - انتظر رسالة "Write Successful".
  - إذا فشلت الكتابة، سجّل السبب (مثل "القطاع محمي" أو "الرقاقة مقفلة").
- **التحقق من التغيير**:
  - انقر "Read" في NFC Tools.
  - ضع الرقاقة خلف الهاتف.
  - تحقق من ظهور "Ali" في القطاع 2 (الكتلة 0 عادةً).
  - التقط لقطة شاشة.
- **تسجيل النتائج**:
  - دوّن:
    - UID.
    - القطاع المستخدم (مثل القطاع 2).
    - النتيجة (مثل "كتبت 'Ali' بنجاح" أو "فشلت بسبب التشفير").
    - أي مشكلات (مثل "القطاع 2 كان محميًا، استخدمت القطاع 3").
  - أرفق لقطة الشاشة.
- **تحليل النتائج**:
  - اكتب فقرة (150-200 كلمة):
    - وصف العملية.
    - هل نجحت الكتابة؟ لماذا؟
    - ما تعلمته (مثل قيود القطاعات المحمية).
  - مثال: "حاولت تغيير بيانات القطاع 2 في رقاقة MIFARE Classic 1K باستخدام NFC Tools. قرأت الرقاقة أولًا لتحديد القطاعات غير المحمية، ووجدت القطاع 2 متاحًا. كتبت الاسم 'Ali' بنجاح في الكتلة 0، وأكدت القراءة ظهور النص. واجهت مشكلة عند محاولة الكتابة في القطاع 1 بسبب الحماية (مطلوب مفتاح). استخدمت MTools لتأكيد أن القطاع 1 محمي بمفتاح غير معروف. تعلمت أن تحديد القطاعات غير المحمية ضروري قبل الكتابة، وأن NFC Tools محدود في التعامل مع الرقائق المشفرة. العملية أوضحت أهمية اختبار الرقاقة مسبقًا."

معايير النجاح:

- تحديد قطاع غير محمي.
- كتابة بيانات جديدة (أو محاولة).
- التحقق من التغيير.
- تسجيل النتائج مع لقطة شاشة.

صورة توضيحية:

- لقطة شاشة: نتيجة القراءة تُظهر "Ali" في القطاع 2.
- تعليق: "مخطط 5.2: تغيير بيانات قطاع غير محمي باستخدام NFC Tools."

تحدي إضافي:

- جرب تغيير بيانات في قطاع آخر.
- إذا كانت جميع القطاعات محمية، استخدم MTools لمحاولة فتح قطاع بمفتاح افتراضي.

5.4 إرشادات الأمان عند التغيير

- **تحقق من القانونية:** لا تُعدّل بطاقات حساسة (مثل بطاقات دفع).
- **استخدم رقائق تجريبية:** مثل Gen1/CUID Magic Cards.
- **سجّل المفاتيح:** احتفظ بنسخة من المفاتيح قبل التعديل.
- **اختبر الرقاقة:** تأكد من أنها غير مقفلة نهائيًا.
- **حماية البيانات:** لا تكتب بيانات حساسة (مثل أرقام بطاقات) على رقائق غير مشفرة.

مخطط ASCII لعملية تغيير البيانات:

```
+-----------------------------------------+
|        عملية تغيير بيانات RFID         |
+-----------------------------------------+
| [اختبار الرقاقة]                        |
| | قراءة UID، تحديد القطاعات             |
| v                                       |
| [تحديد القطاع]                          |
| | اختر قطاعًا غير محمي                  |
| v                                       |
| [كتابة البيانات]                        |
| | (مثل "1234" أو "Ali")                 |
| v                                       |
| [التحقق]                                |
| | قراءة الرقاقة، تأكيد البيانات         |
| v                                       |
| [تسجيل النتائج]                         |
| | (نجاح/فشل، لقطة شاشة)                 |

+-----------------------------------------+
```

- **شرح المخطط:**
  - يوضح خطوات تغيير البيانات من الاختبار إلى التسجيل.
- **الصورة في الكتاب:**
  - رسم تدفقي: اختبار → تحديد → كتابة → تحقق.
  - تعليق: "مخطط 5.3: عملية تغيير البيانات تتطلب تحديد قطاع غير محمي."

ملخص الفصل

- تغيير بيانات RFID يتطلب أدوات (NFC Tools، MTools) ورقائق قابلة للكتابة.
- كتابة رقم جديد (مثل "1234") على MIFARE Classic ممكن إذا كانت الرقاقة غير محمية.
- تغيير بيانات القطاعات غير المحمية ينجح عادةً، لكن الرقائق المشفرة تحتاج إلى مفاتيح.
- الأمان ضروري لتجنب إفساد الرقاقة أو انتهاك القوانين.

أسئلة مراجعة

- ما الخطوات الأساسية لكتابة رقم جديد على MIFARE Classic؟
- لماذا قد تفشل كتابة البيانات في قطاع معين؟
- كيف تتحقق من نجاح تغيير البيانات؟
- ما دور MTools في التعامل مع الرقائق المحمية؟
- كيف تؤثر إعدادات الحماية على عملية التغيير؟

موارد إضافية

- **فيديوهات**:
  - "كتابة بيانات على MIFARE Classic" (youtube.com/mifare-write (#)).
  - "تغيير بيانات RFID بأمان" (youtube.com/rfid-change-safety (#)).
- **موقع**: rfid-guide.x.ai.
- **تطبيقات**: NFC Tools، MTools.
- **وثائق**:
  - دليل MIFARE Classic: www.mifare.net.

الفصل السادس: تقنيات متقدمة

أهداف الفصل

- استكشاف تقنيات متقدمة في RFID مثل البرمجة باستخدام Arduino وRC522.
- تعلم كيفية قراءة وكتابة البيانات على رقائق RFID باستخدام أكواد Arduino.
- فهم كيفية دمج RFID مع أنظمة أخرى (مثل قواعد البيانات أو IoT).
- تقديم تمرين عملي لبرمجة RC522.
- توفير وصف فيديو لتوصيل RC522 وتشغيل الكود.

6.1 مقدمة عن التقنيات المتقدمة

التقنيات المتقدمة في RFID تشمل البرمجة المخصصة، إدارة البيانات، والتكامل مع أنظمة مثل Arduino، Raspberry Pi، أو السحابة. هذا الفصل يركز على استخدام وحدة RC522 (MFRC522) مع Arduino لقراءة وكتابة البيانات على رقائق MIFARE Classic 1K/4K. RC522 هي وحدة RFID شائعة تعمل على تردد 13.56 ميجاهرتز، تدعم بروتوكول ISO/IEC 14443 A، وتُستخدم في تطبيقات مثل التحكم في الوصول وتتبع الأصول.

6.1.1 مكونات RC522

- **MFRC522 IC**: دائرة مدمجة للقراءة/الكتابة بدون تلامس.

- **الهوائي**: يولد حقلًا كهرومغناطيسيًا بتردد 13.56 ميجاهرتز.
- **الواجهات**: SPI (الأكثر شيوعًا)، UART، I2C.
- **الجهد**: 2.5-3.3 فولت (دبابيس الاتصال تتحمل 5 فولت).
- **الرقائق المدعومة**: MIFARE Classic، Ultralight، NTAG.

6.1.2 أهمية البرمجة

- **القراءة**: استخراج UID أو بيانات القطاعات.
- **الكتابة**: تخزين بيانات مخصصة (مثل أسماء، أرقام).
- **التكامل**: ربط RFID مع قواعد بيانات أو تطبيقات IoT.
- **الأمان**: إدارة المفاتيح للرقائق المحمية.

6.2 إعداد RC522 مع Arduino

الوصف: RC522 تتصل بـ Arduino عبر واجهة SPI، مما يتيح قراءة وكتابة البيانات بسهولة باستخدام مكتبة MFRC522. هذا القسم يشرح التوصيلات، تثبيت المكتبة، وكتابة الأكواد.

الأدوات المطلوبة:

- لوحة Arduino (Uno/Nano/Mega).
- وحدة RC522 مع بطاقة MIFARE Classic 1K.
- أسلاك توصيل (Jumper Wires).
- لوح تجارب (Breadboard).
- جهاز كمبيوتر مع Arduino IDE.

التوصيلات:

دبوس RC522	دبوس Arduino Uno	الوصف
VCC	3.3V	مصدر الطاقة (تحذير: 5V قد يتلف الوحدة)
GND	GND	الأرضي
RST	9	إعادة تعيين
SDA (SS)	10	اختيار العبد (Slave Select)
MOSI	11	Master Out Slave In
MISO	12	Master In Slave Out
SCK	13	ساعة SPI
IRQ	غير متصل	مقاطعة (اختياري)

ملاحظات التوصيل:

- تأكد من استخدام 3.3V لـ VCC لتجنب إتلاف RC522.
- استخدم أسلاك قصيرة لتقليل التداخل في SPI.
- إذا استخدمت Arduino Mega، راجع التوصيلات المختلفة (مثل SDA إلى 53).

مخطط التوصيل (ASCII):

```
Arduino Uno      RC522
+-----------+    +-----------+
|      3.3V  ----+----| VCC |
|      GND   ----+----| GND |
|       D9    ----+----| RST |
| (D10   ----+----| SDA (SS |
|      D11   ----+----| MOSI |
|      D12   ----+----| MISO |
|      D13   ----+----| SCK |
+-----------+    +-----------+
```

- **الصورة في الكتاب**: رسم تخطيطي ملون يوضح التوصيلات على لوح تجارب (مخطط 6.1: توصيل RC522 بـ Arduino Uno).

تثبيت مكتبة MFRC522:

- افتح Arduino IDE.
- انتقل إلى **Sketch → Include Library → Manage Libraries**.
- ابحث عن "MFRC522"، ثم ثبت المكتبة بواسطة GithubCommunity.
- تحقق من توفر أمثلة المكتبة عبر **File → Examples → MFRC522**.

6.3 تمرين: برمجة RC522 لقراءة/كتابة

الهدف: برمجة RC522 لقراءة UID وبيانات رقاقة MIFARE Classic 1K، ثم كتابة نص مخصص (مثل "Student123") إلى القطاع 1، والتحقق من الكتابة.

الأدوات المطلوبة:

- نفس الأدوات المذكورة في 6.2.
- بطاقة MIFARE Classic 1K (يفضل Gen1/CUID غير محمية).
- دفتر ملاحظات لتسجيل النتائج.

الخطوات:

- **قراءة UID وبيانات الرقاقة:**
  - **الكود** (مستند إلى DumpInfo من مكتبة MFRC522):
  - cpp

```
<include <SPI.h#
<include <MFRC522.h#
define RST_PIN 9#
define SS_PIN 10#
;(MFRC522 rfid(SS_PIN, RST_PIN
} ()void setup
;(Serial.begin(9600
;()SPI.begin
;()rfid.PCD_Init
;("...Serial.println("Tap an RFID card
{
```

```
} ()void loop
} (()if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial
;return
{
;(" :Serial.print("Card UID
} (++for (byte i = 0; i < rfid.uid.size; i
;(" " : "Serial.print(rfid.uid.uidByte[i] < 0x10 ? " 0
;(Serial.print(rfid.uid.uidByte[i], HEX
{
;()Serial.println
;(MFRC522::PICC_Type piccType = rfid.PICC_GetType(rfid.uid.sak
;(" :Serial.print("PICC Type
;((Serial.println(rfid.PICC_GetTypeName(piccType
تفريغ بيانات الرقاقة // ;((rfid.PICC_DumpToSerial(&(rfid.uid
;()rfid.PICC_HaltA
;()rfid.PCD_StopCrypto1
```

- {
- **الشرح**:
  - يُهيئ الكود واجهة SPI وRC522.
  - عند اقتراب بطاقة، يقرأ UID ونوع الرقاقة (مثل MIFARE Classic 1K).
  - PICC_DumpToSerial يعرض خريطة الذاكرة (القطاعات والكتل).
  - يُستخدم مفتاح افتراضي (FFFFFFFFFFFF) للقطاعات المحمية.
- **التشغيل**:
  - قم بتوصيل RC522 كما في 6.2.
  - ارفع الكود إلى Arduino.
  - افتح Serial Monitor (115200 baud).
  - ضع البطاقة أمام القارئ.
  - سجل UID (مثل "A1 B2 C3 04") ونوع الرقاقة.
  - دوّن خريطة الذاكرة (مثل القطاع 1، الكتلة 0).

- **كتابة نص إلى القطاع 1**:
  - **الكود** (لكتابة "Student123" إلى القطاع 1، الكتلة 0):
  - cpp

```
<include <SPI.h#
<include <MFRC522.h#
define RST_PIN 9#
define SS_PIN 10#
;(MFRC522 rfid(SS_PIN, RST_PIN
;MFRC522::MIFARE_Key key
;"byte data[16] = "Student123
} ()void setup
;(Serial.begin(9600
;()SPI.begin
;()rfid.PCD_Init
} (++for (byte i = 0; i < 6; i
```

```
    key.keyByte[i] = 0xFF; // مفتاح افتراضي
  }
  Serial.println("Tap an RFID card to write...");
}
void loop() {
  if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial()) {
    return;
  }
  Serial.println("Card detected, writing data...");
  byte sector = 1;
  byte block = 4; // الكتلة 0 في القطاع 1
  MFRC522::StatusCode status;
  status = rfid.PCD_Authenticate(MFRC522::PICC_CMD_MF_AUTH_KEY_A, block, &key, &(rfid.uid));
  if (status != MFRC522::STATUS_OK) {
    Serial.print("Authentication failed: ");
    Serial.println(rfid.GetStatusCodeName(status));
    return;
  }
  status = rfid.MIFARE_Write(block, data, 16);
  if (status != MFRC522::STATUS_OK) {
    Serial.print("Write failed: ");
    Serial.println(rfid.GetStatusCodeName(status));
    return;
  }
  Serial.println("Data written successfully!");
  rfid.PICC_HaltA();
  rfid.PCD_StopCrypto1();
```

- }
- **الشرح**:
  - يُهيئ الكود RC522 ويحدد مفتاحًا افتراضيًا (FFFFFFFFFFFF).
  - يصادق على القطاع 1 باستخدام مفتاح A.
  - يكتب "Student123" إلى الكتلة 4 (الكتلة 0 في القطاع 1).
  - يتحقق من نجاح الكتابة عبر Serial Monitor.
- **التشغيل**:
  - ارفع الكود إلى Arduino.
  - ضع البطاقة أمام القارئ.
  - تحقق من رسالة "Data written successfully!" في Serial Monitor.
  - إذا فشلت الكتابة (مثل "Authentication failed")، تحقق من المفتاح أو حالة القطاع.

- **التحقق من الكتابة**:
  - استخدم الكود الأول (DumpInfo) لقراءة البطاقة.
  - تحقق من ظهور "Student123" في القطاع 1، الكتلة 0.
  - التقط لقطة شاشة لـ Serial Monitor.
- **تسجيل النتائج**:
  - دوّن:

- UID.
- نوع الرقاقة.
- نتيجة القراءة (مثل "UID: 04 A1 B2 C3").
- نتيجة الكتابة (مثل "كتبت Student123 بنجاح").
- أي مشكلات (مثل "فشل المصادقة بسبب مفتاح غير صحيح").
- أرفق لقطة شاشة لـ Serial Monitor.
- اكتب فقرة تحليلية (150-200 كلمة):
  - وصف العملية.
  - هل نجحت الكتابة؟ لماذا؟
  - ما تعلمته (مثل أهمية المفتاح أو قيود RC522).
- مثال: "برمجت RC522 لقراءة UID وكتابة 'Student123' إلى القطاع 1 باستخدام Arduino Uno. قرأت UID بنجاح ('A1 B2 C3 04') باستخدام DumpInfo، ثم كتبت النص إلى الكتلة 4 بعد المصادقة بمفتاح افتراضي. الكتابة نجحت، وأكدت القراءة ظهور 'Student123'. واجهت مشكلة أولية بسبب مفتاح غير صحيح، لكن استخدام 'FFFFFFFFFFFF' حلها. تعلمت أن RC522 سهلة البرمجة مع مكتبة MFRC522، لكن القطاعات المحمية تتطلب مفاتيح دقيقة. SPI يحتاج إلى توصيلات قصيرة لتجنب الأخطاء."

معايير النجاح:

- قراءة UID وبيانات الرقاقة بنجاح.
- كتابة "Student123" إلى القطاع 1.
- التحقق من الكتابة.
- تسجيل النتائج مع لقطة شاشة.

صورة توضيحية:

- لقطة شاشة: Serial Monitor يُظهر "Student123" في القطاع 1.
- تعليق: "مخطط 6.2: كتابة نص مخصص إلى MIFARE Classic باستخدام RC522."

تحدي إضافي:

- جرب كتابة نص إلى قطاع آخر (مثل القطاع 2).
- أضف شرطًا في الكود للتحقق من UID قبل الكتابة (مثل "فقط إذا كان UID = 04 A1 B2 C3").

6.4 فيديو: توصيل RC522 وتشغيل الكود

الوصف: فيديو تعليمي مدته 5-7 دقائق يوضح توصيل RC522 بـ Arduino Uno، رفع الكود، وقراءة/كتابة بيانات.
محتوى الفيديو:

- **المقدمة (0:00-0:30):**
  - شرح موجز لـ RC522 واستخداماتها.
  - قائمة المكونات (RC522، Arduino Uno، بطاقة MIFARE).
- **التوصيل (0:30-2:00):**
  - عرض لوح التجارب مع Arduino وRC522.
  - توصيل الأسلاك خطوة بخطوة (VCC → 3.3V، GND → GND، إلخ).
  - تحذير: "لا تستخدم 5V لـ VCC لتجنب إتلاف الوحدة."
- **إعداد Arduino IDE (2:00-3:30):**

- تثبيت مكتبة MFRC522.
- فتح مثال DumpInfo.
- ضبط Serial Monitor على baud 115200.
- **تشغيل الكود (3:30-5:00)**:
  - رفع كود DumpInfo.
  - وضع بطاقة أمام القارئ.
  - عرض UID وخريطة الذاكرة في Serial Monitor.
  - رفع كود الكتابة (من التمرين).
  - كتابة "Student123" والتحقق.
- **الخاتمة (5:00-5:30)**:
  - ملخص الخطوات.
  - دعوة لتجربة مشاريع مثل قفل الأبواب.

إعداد الفيديو:

- **الكاميرا**: كاميرا واضحة (1080p) تُظهر لوح التجارب.
- **الصوت**: ميكروفون واضح مع شرح بطيء.
- **التعليقات**: نصوص توضيحية (مثل "VCC → 3.3V").
- **البرمجيات**: Arduino IDE، Serial Monitor.
- **الإضاءة**: إضاءة جيدة لإظهار التوصيلات.

رابط الفيديو (افتراضي): youtube.com/rc522-arduino-demo (#).

- **الصورة في الكتاب**: لقطة من الفيديو تُظهر التوصيلات (مخطط 6.3: إعداد RC522 في الفيديو).

6.5 تقنيات متقدمة أخرى

- **إدارة المفاتيح**: تغيير مفاتيح القطاعات باستخدام MTools أو Arduino.
- **التكامل مع IoT**: إرسال بيانات RFID إلى السحابة (مثل Blynk).
- **الأمان**: تشفير البيانات باستخدام MIFARE DESFire.
- **متعدد القارئات**: إدارة عدة RC522 مع Arduino Mega.

مخطط ASCII لعملية البرمجة:

```
+------------------------------------------+
|              عملية برمجة RC522            |
+------------------------------------------+
| [إعداد التوصيلات]               |
| | VCC → 3.3V, GND, SPI            |
|  v                          |
| [تثبيت المكتبة]                 |
| | MFRC522 عبر Arduino IDE         |
|  v                          |
| [رفع الكود]                     |
| | DumpInfo أو كود الكتابة          |
|  v                          |
| [اختبار القراءة]                 |
```

```
| | UID، خريطة الذاكرة           |
|   v                                 |
| [اختبار الكتابة]                 |
| | "Student123" إلى القطاع 1     |
+------------------------------------------+
```

- **الصورة في الكتاب**: رسم تدفقي ملون (مخطط 6.4: تدفق برمجة RC522).

ملخص الفصل

- RC522 هي وحدة RFID قوية وسهلة البرمجة مع Arduino.
- مكتبة MFRC522 تُبسط القراءة والكتابة.
- التوصيلات الحساسة (مثل 3.3V) تتطلب دقة.
- التقنيات المتقدمة تشمل إدارة المفاتيح والتكامل مع IoT.

أسئلة مراجعة

- ما الفرق بين SPI وI2C في RC522؟
- لماذا يجب استخدام 3.3V لـ VCC؟
- كيف تتحقق من نجاح كتابة البيانات؟
- ما دور مفتاح المصادقة في MIFARE Classic؟
- كيف يمكن دمج RC522 مع السحابة؟

الفصل السابع: التطبيقات العملية

أهداف الفصل

- استكشاف تطبيقات RFID العملية (مثل تتبع المخزون، التحكم في الوصول).
- تصميم مخططات لسيناريوهات عملية.
- تقديم تمرين لتصميم نظام RFID بسيط.
- توفير أمثلة واقعية مع تحليل.

7.1 مقدمة عن التطبيقات العملية

RFID تُستخدم في صناعات متعددة مثل اللوجستيات، التجزئة، والأمن. هذا الفصل يركز على تطبيقات عملية يمكن تنفيذها باستخدام RC522 أو NFC Tools، مع التركيز على تصميم أنظمة بسيطة وقابلة للتطوير.

7.1.1 أمثلة التطبيقات

- **تتبع المخزون**: مراقبة المنتجات في المستودعات.
- **التحكم في الوصول**: قفل أبواب ببطاقات RFID.
- **الحضور الآلي**: تسجيل حضور الطلاب/الموظفين.
- **الدفع بدون تلامس**: محاكاة بطاقات الدفع.
- **مكافحة السرقة**: تتبع الأصول في المتاجر.

7.2 مخططات لسيناريوهات عملية

الوصف: يقدم هذا القسم مخططات لسيناريوهات RFID مع شرح للمكونات والتطبيق.

- **سيناريو 1: تتبع المخزون**
  - **الوصف**: نظام لتتبع المنتجات في مستودع باستخدام RC522 وArduino.
  - **المكونات**:
    - Arduino Uno.
    - RC522.
    - بطاقات MIFARE Classic (واحدة لكل منتج).
    - شاشة LCD (لعرض UID والمنتج).
    - برنامج قاعدة بيانات (مثل Excel أو MySQL).
  - **آلية العمل**:
    - كل منتج مزود ببطاقة RFID تحتوي على معرف المنتج (مثل "PROD001").
    - عند المرور عبر القارئ، يقرأ Arduino UID ويطابق المعرف في قاعدة البيانات.
    - تُحدّث حالة المخزون (مثل "في المستودع" أو "مُشحن").
  - **مخطط ASCII**:

```
+-----------------+
| منتج + بطاقة    |
| (PROD001)       |
+-----------------+
        |
        v
+-----------------+
| RC522 Reader    |
| (قراءة UID)     |
+-----------------+
        |
        v
+-----------------+
| Arduino Uno     |
| (معالجة UID)    |
+-----------------+
        |
        v
+-----------------+
| LCD / Database  |
| (عرض/تخزين)     |
```

  - +-----------------+
  - **الصورة في الكتاب**: رسم تخطيطي يوضح تدفق البيانات من البطاقة إلى قاعدة البيانات (مخطط 7.1: نظام تتبع المخزون).
- **سيناريو 2: التحكم في الوصول**
  - **الوصف**: قفل باب يفتح فقط لبطاقات RFID مُصرح لها.
  - **المكونات**:
    - Arduino Uno.

- RC522.
- مرحل (Relay) للتحكم في القفل.
- بطاقات RFID (مثل "USER001").

- **آلية العمل**:
  - يقرأ RC522 UID.
  - يقارن Arduino UID مع قائمة البطاقات المصرح لها.
  - إذا تطابقت، يُفعّل المرحل لفتح القفل.
- **مخطط ASCII**:

```
+-----------------+
| بطاقة RFID |
| (USER001) |
+-----------------+
        |
        v
+-----------------+
| RC522 Reader |
| (قراءة UID) |
+-----------------+
        |
        v
+-----------------+
| Arduino Uno |
| (التحقق) |
+-----------------+
        |
        v
+-----------------+
| Relay / Lock |
| (فتح/قفل) |
```

- +-----------------+
- **الصورة في الكتاب**: رسم يوضح البطاقة، القارئ، والقفل (مخطط 7.2: نظام التحكم في الوصول).

7.3 تمرين: تصميم نظام RFID بسيط

الهدف: تصميم نظام RFID لتتبع حضور الطلاب باستخدام RC522 وArduino، مع عرض UID واسم الطالب على Serial Monitor.

الأدوات المطلوبة:

- Arduino Uno.
- RC522.
- بطاقات MIFARE Classic (واحدة لكل طالب).
- جهاز كمبيوتر مع Arduino IDE.

الخطوات:

- **إعداد النظام:**
  - قم بتوصيل RC522 كما في 6.2.
  - ثبت مكتبة MFRC522.
- **كتابة الكود:**
  - **الكود:**
  - cpp

```cpp
#include <SPI.h>
#include <MFRC522.h>
#define RST_PIN 9
#define SS_PIN 10
MFRC522 rfid(SS_PIN, RST_PIN);
String authorizedCards[] = {"04 A1 B2 C3", "05 D4 E5 F6"};
String studentNames[] = {"Ali Ahmed", "Sara Mohammed"};
void setup() {
  Serial.begin(9600);
  SPI.begin();
  rfid.PCD_Init();
  Serial.println("Student Attendance System");
  Serial.println("Tap an RFID card...");
}
void loop() {
  if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial()) {
    return;
  }
  String uid = "";
  for (byte i = 0; i < rfid.uid.size; i++) {
    uid += String(rfid.uid.uidByte[i] < 0x10 ? "0" : "");
    uid += String(rfid.uid.uidByte[i], HEX);
    if (i < rfid.uid.size - 1) uid += " ";
  }
  uid.toUpperCase();
  bool authorized = false;
  for (int i = 0; i < 2; i++) {
    if (uid == authorizedCards[i]) {
      Serial.print("Welcome, ");
      Serial.println(studentNames[i]);
      authorized = true;
      break;
    }
  }
  if (!authorized) {
    Serial.println("Unauthorized card!");
  }
  rfid.PICC_HaltA();
  delay(2000);
```

- }
- **الشرح:**
  - يخزن الكود قائمة بـ UID وأسماء الطلاب.
  - عند قراءة بطاقة، يقارن UID مع القائمة.
  - إذا تطابقت، يعرض اسم الطالب (مثل "Welcome, Ali Ahmed").
  - إذا لم تتطابق، يعرض "Unauthorized card!".
- **اختبار النظام:**
  - ارفع الكود إلى Arduino.
  - ضع بطاقة مُصرح لها (مثل "A1 B2 C3 04").
  - تحقق من ظهور الاسم في Serial Monitor.
  - جرب بطاقة غير مُصرح لها.
- **تسجيل النتائج:**
  - دوّن:
    - UID لكل بطاقة.
    - النتيجة (مثل "Ali Ahmed ظهر بنجاح").
    - أي مشكلات (مثل "تأخير في القراءة").
  - التقط لقطة شاشة لـ Serial Monitor.
  - اكتب فقرة تحليلية (150-200 كلمة):
    - وصف النظام.
    - هل نجح؟ لماذا؟
    - ما تعلمته.
  - مثال: "صممت نظام حضور باستخدام RC522 وArduino Uno. النظام يقرأ UID ويعرض اسم الطالب إذا كان مُصرحًا. اختبرت بطاقتين: الأولى ('A1 B2 C3 04') أظهرت 'Welcome, Ali Ahmed'، والثانية (غير مُصرح لها) أظهرت 'Unauthorized card!'. الكود عمل بسلاسة، لكن واجهت تأخيرًا طفيفًا عند قراءة البطاقة بسبب المسافة. تعلمت أن RC522 فعالة لتتبع الحضور، لكن يجب ضبط حساسية الهوائي. النظام قابل للتطوير بإضافة قاعدة بيانات."

معايير النجاح:

- تصميم نظام يعرض أسماء الطلاب المُصرح لهم.
- اختبار البطاقات المُصرح لها وغير المُصرح لها.
- تسجيل النتائج مع لقطة شاشة.

صورة توضيحية:

- لقطة شاشة: Serial Monitor يُظهر "Welcome, Ali Ahmed".
- تعليق: "مخطط 7.3: نظام تتبع الحضور باستخدام RC522."

تحدي إضافي:

- أضف LED يضيء عند تسجيل حضور مُصرح.
- قم بتخزين بيانات الحضور في ملف على بطاقة SD.

ملخص الفصل

- RFID تُستخدم في تتبع المخزون، التحكم في الوصول، والحضور.
- المخططات تُبسط تصميم الأنظمة.
- نظام الحضور باستخدام RC522 بسيط وقابل للتطوير.

أسئلة مراجعة

- ما الفائدة من تتبع المخزون باستخدام RFID؟
- كيف يعمل نظام التحكم في الوصول؟
- ما المكونات الأساسية لنظام حضور RFID؟
- كيف يمكن تحسين نظام الحضور؟
- ما التحديات في تصميم أنظمة RFID؟

الفصل الثامن: الجوانب القانونية والأخلاقية

أهداف الفصل

- فهم الجوانب القانونية والأخلاقية لاستخدام RFID.
- تقديم رسوم توضيحية للاستخدام القانوني مقابل غير القانوني.
- تمرين لمناقشة سيناريو أخلاقي.
- مناقشة الخصوصية والأمان.

8.1 مقدمة عن الجوانب القانونية والأخلاقية

RFID تثير قضايا قانونية وأخلاقية تتعلق بالخصوصية، الأمان، والاستخدام غير المصرح به. هذا الفصل يناقش القوانين (مثل GDPR في أوروبا)، المخاوف الأخلاقية (مثل تتبع الأفراد)، وكيفية ضمان الاستخدام المسؤول.

8.1.1 القضايا القانونية

- **الخصوصية**: جمع البيانات دون موافقة (ممنوع في GDPR).
- **الأمان**: حماية بيانات RFID من القرصنة.
- **التزوير**: تعديل بطاقات RFID (مثل بطاقات الدفع) غير قانوني.
- **اللوائح**: تختلف حسب الدولة (مثل FCC في الولايات المتحدة).

8.1.2 القضايا الأخلاقية

- **تتبع الأفراد**: قد يُعتبر انتهاكًا للخصوصية.
- **شفافية**: إبلاغ المستخدمين باستخدام RFID.
- **إساءة الاستخدام**: مثل نسخ بطاقات الوصول.

8.2 رسوم توضيحية للاستخدام القانوني مقابل غير القانوني

الوصف: رسوم توضيحية تُظهر أمثلة على الاستخدام القانوني (مثل تتبع المخزون) وغير القانوني (مثل نسخ بطاقة دفع).

- **الاستخدام القانوني**:
  - **مثال**: نظام تتبع المخزون في مستودع.
  - **الوصف**: بطاقات RFID على المنتجات تُقرأ بموافقة الشركة، مع تشفير البيانات.
  - **الرسم التوضيحي**:

```
+-----------------+
| منتج + بطاقة |
| (مشفرة)      |
+-----------------+
        |
        v
+-----------------+
| قارئ RFID      |
| (معتمد)       |
+-----------------+
        |
        v
+-----------------+
| قاعدة بيانات |
| (محمية)       |
```

- +-----------------+
- **الصورة في الكتاب**: رسم ملون يوضح قارئ RFID يقرأ بطاقة مشفرة مع رمز قفل (مخطط 8.1: الاستخدام القانوني).
- **الاستخدام غير القانوني**:
- **مثال**: نسخ بطاقة دفع بدون إذن.
- **الوصف**: استخدام قارئ RFID لنسخ بيانات بطاقة دفع لاستخدامها في عمليات احتيال.
- **الرسم التوضيحي**:

```
+-----------------+
| بطاقة دفع    |
| (غير محمية)  |
+-----------------+
        |
        v
+-----------------+
| قارئ غير مصرح |
| (Proxmark3)    |
+-----------------+
        |
        v
+-----------------+
| بطاقة مزيفة   |
| (احتيال)      |
```

- +-----------------+
- **الصورة في الكتاب**: رسم يوضح قارئ غير مصرح مع رمز تحذير (مخطط 8.2: الاستخدام غير القانوني).

8.3 تمرين: مناقشة سيناريو أخلاقي

الهدف: مناقشة سيناريو أخلاقي حول استخدام RFID وكتابة تقرير تحليلي.
السيناريو:

- شركة تستخدم RFID لتتبع موظفيها داخل المكتب دون إبلاغهم. البيانات تُستخدم لتحسين الإنتاجية، لكن الموظفون يشعرون بانتهاك خصوصيتهم.

الخطوات:

- **تحليل السيناريو**:
  - اكتب فقرة (200-250 كلمة) تجيب على:
    - هل الاستخدام قانوني؟ (راجع GDPR أو قوانين محلية).
    - هل هو أخلاقي؟ لماذا؟
    - ما الحلول لتحسين الوضع؟
  - مثال: "استخدام RFID لتتبع الموظفين دون موافقة قد يكون غير قانوني بموجب GDPR، الذي يتطلب موافقة صريحة لجمع البيانات الشخصية. أخلاقيًا، هو انتهاك للخصوصية لأن الموظفين لم يُبلغوا، مما يقلل الثقة. الحلول تشمل: إبلاغ الموظفين وشرح الفوائد (مثل تحسين الأمان)، تشفير البيانات، وإتاحة خيار الرفض. تعلمت أن الشفافية ضرورية للاستخدام الأخلاقي لـ RFID."
- **مناقشة جماعية** (اختياري):
  - ناقش السيناريو مع زملاء (إذا كنت في فصل دراسي).
  - سجل وجهات النظر المختلفة.
- **تسجيل النتائج**:
  - أرفق الفقرة التحليلية.
  - أضف ملاحظات المناقشة (إن وجدت).

معايير النجاح:

- تحليل قانوني وأخلاقي دقيق.
- اقتراح حلول عملية.
- كتابة فقرة واضحة.

صورة توضيحية:

- رسم بياني يقارن بين الاستخدام الشفاف (مع موافقة) وغير الشفاف (بدون موافقة).
- تعليق: "مخطط 8.3: الشفافية في استخدام RFID."

تحدي إضافي:

- ابحث عن قانون محلي ينظم RFID وناقش تأثيره على السيناريو.

ملخص الفصل

- RFID تثير قضايا قانونية (خصوصية، أمان) وأخلاقية (شفافية).
- الاستخدام القانوني يتطلب موافقة وتشفير.
- المناقشات الأخلاقية تُعزز المسؤولية.

أسئلة مراجعة

- ما القوانين التي تنظم استخدام RFID؟

- لماذا تُعتبر الشفافية مهمة؟
- كيف يمكن حماية بيانات RFID؟
- ما أمثلة على الاستخدام غير القانوني؟
- كيف تؤثر الأخلاق على تصميم أنظمة RFID؟

الفصل التاسع: استكشاف الأخطاء وإصلاحها

أهداف الفصل

- تعلم كيفية تشخيص وإصلاح مشكلات RFID الشائعة.
- تقديم صور لأخطاء شائعة (مثل شاشة خطأ في NFC Tools).
- تمرين لمحاولة إصلاح مشكلة اتصال.
- توفير نصائح وقائية.

9.1 مقدمة عن استكشاف الأخطاء

مشكلات RFID تشمل فشل الاتصال، أخطاء القراءة/الكتابة، والتداخل. هذا الفصل يقدم دليلًا لتشخيص الأخطاء وإصلاحها، مع التركيز على RC522 وNFC Tools.

9.1.1 الأخطاء الشائعة

- **فشل الاتصال**: القارئ لا يستجيب (مثل "Communication failure" في RC522).
- **أخطاء القراءة**: القارئ لا يكتشف البطاقة.
- **أخطاء الكتابة**: فشل الكتابة بسبب الحماية.
- **التداخل**: إشارات متداخلة تؤثر على الأداء.

9.2 صور لأخطاء شائعة

الوصف: صور توضح رسائل الخطأ ومشكلات الأجهزة مع حلول مقترحة.

- **خطأ في NFC Tools**:
  - **الصورة**: لقطة شاشة تُظهر "Tag is Locked" في واجهة الكتابة.
  - **السبب**: الرقاقة مقفلة نهائيًا أو محمية بمفتاح غير معروف.
  - **الحل**:
    - استخدم MTools لإدخال مفتاح (مثل "FFFFFFFFFFFF").
    - جرب رقاقة جديدة (مثل Gen1/CUID).
  - **الصورة في الكتاب**: لقطة شاشة مع تعليق "مخطط 9.1: خطأ 'Tag is Locked' في NFC Tools."
- **خطأ في RC522**:
  - **الصورة**: Serial Monitor يُظهر "WARNING: Communication failure, is the MFRC522 properly connected?".
  - **السبب**: توصيلات غير صحيحة، جهد غير مناسب، أو لحام رديء.
  - **الحل**:
    - تحقق من التوصيلات (VCC → 3.3V، SDA → 10).
    - استخدم أسلاك قصيرة ولوح تجارب نظيف.
    - أضف مكثف (100nF) بين VCC وGND لتثبيت الجهد.
  - **الصورة في الكتاب**: لقطة شاشة مع تعليق "مخطط 9.2: خطأ اتصال RC522."

- **خطأ الأجهزة**:
  - **الصورة**: صورة لوح تجارب تُظهر أسلاكًا مفكوكة.
  - **السبب**: لحام رديء أو أسلاك طويلة.
  - **الحل**:
    - أعد اللحام أو استخدم لوحة PCB.
    - قلل طول الأسلاك.
  - **الصورة في الكتاب**: صورة مع تعليق "مخطط 9.3: مشكلة توصيلات RC522."

9.3 تمرين: محاولة إصلاح مشكلة اتصال

الهدف: تشخيص وإصلاح مشكلة اتصال في RC522 تُظهر "Communication failure" في Serial Monitor.
الأدوات المطلوبة:

- Arduino Uno.
- RC522.
- جهاز كمبيوتر مع Arduino IDE.
- أسلاك توصيل ولوح تجارب.

الخطوات:

- **إعادة إنتاج المشكلة**:
  - قم بتوصيل RC522 كما في 6.2.
  - ارفع كود DumpInfo (من 6.3).
  - افتح Serial Monitor.
  - إذا ظهر "Communication failure"، تابع.
- **التشخيص**:
  - تحقق من التوصيلات:
    - VCC → 3.3V؟
    - SDA → 10؟
    - RST → 9؟
  - تحقق من الجهد:
    - استخدم مقياس جهد للتأكد من 3.3V على VCC.
  - تحقق من الأسلاك:
    - هل هناك أسلاك مفكوكة أو طويلة؟
  - تحقق من مصدر الطاقة:
    - هل USB يوفر تيارًا كافيًا؟ جرب مصدر طاقة خارجي.
- **الإصلاح**:
  - أعد توصيل الأسلاك إذا لزم الأمر.
  - استبدل الأسلاك الطويلة بأخرى قصيرة.
  - أضف مكثف 100nF بين VCC وGND.
  - ارفع الكود مرة أخرى.
  - اختبر ببطاقة MIFARE.
- **تسجيل النتائج**:
  - دوّن:
    - سبب المشكلة (مثل "سلك SDA مفكوك").

- الحل (مثل "استبدلت الأسلاك").
- النتيجة (مثل "قرأت UID بنجاح").
- التقط لقطة شاشة لـ Serial Monitor (مع UID ظاهر).
- اكتب فقرة تحليلية (150-200 كلمة):
  - وصف المشكلة والحل.
  - ما تعلمته.
- مثال: "واجهت خطأ 'Communication failure' عند اختبار RC522. بعد التحقق، وجدت أن سلك SDA مفكوك. أعدت التوصيل واستبدلت الأسلاك الطويلة بأخرى قصيرة، ثم أضفت مكثف 100nF. الكود عمل بعد ذلك، وقرأت UID ('04 A1 B2 C3') بنجاح. تعلمت أن التوصيلات الحساسة في SPI تتطلب أسلاكًا قصيرة وجهدًا مستقرًا. فحص الأسلاك خطوة أساسية قبل اللجوء إلى حلول معقدة."

معايير النجاح:

- تشخيص سبب الخطأ.
- إصلاح المشكلة.
- قراءة UID بنجاح.
- تسجيل النتائج مع لقطة شاشة.

صورة توضيحية:

- لقطة شاشة: Serial Monitor يُظهر UID بعد الإصلاح.
- تعليق: "مخطط 9.4: نجاح قراءة UID بعد إصلاح الاتصال."

تحدي إضافي:

- جرب إصلاح خطأ "Tag is Locked" في NFC Tools.
- اختبر RC522 مع مصدر طاقة خارجي.

ملخص الفصل

- استكشاف الأخطاء يتطلب فحص التوصيلات، الجهد، والأسلاك.
- الأخطاء الشائعة تشمل فشل الاتصال وأخطاء الكتابة.
- النصائح الوقائية تُقلل المشكلات.

أسئلة مراجعة

- ما أسباب "Communication failure" في RC522؟
- كيف تُصلح خطأ "Tag is Locked"؟
- لماذا تُستخدم أسلاك قصيرة في SPI؟
- ما دور المكثف في تثبيت الجهد؟
- كيف تمنع مشكلات RFID؟

الفصل العاشر: مواصلة التعلم

أهداف الفصل

- توجيه القارئ لمواصلة تطوير مهاراته في تقنيات RFID من خلال مصادر تعليمية وعملية.
- تقديم أدوات وموارد مجانية لتحميل برامج RFID وشراء الأجهزة.
- تمكين القارئ من فهم المصطلحات التقنية عبر قاموس شامل.
- توفير قوالب بيانات جاهزة لتطبيقات RFID عملية.
- تعزيز التعلم الذاتي من خلال خطة دراسة ومشاريع مقترحة.
- ربط المحتوى مع الفصول السابقة (مثل برمجة RC522، التطبيقات العملية، والجوانب الأخلاقية).

10.1 مقدمة عن مواصلة التعلم

بعد تغطية أساسيات RFID (الفصل الثاني: هيكلية الرقائق)، الأدوات (الفصل الثالث)، تغيير البيانات (الفصل الخامس)، التقنيات المتقدمة (الفصل السادس)، التطبيقات العملية (الفصل السابع)، الجوانب القانونية والأخلاقية (الفصل الثامن)، واستكشاف الأخطاء (الفصل التاسع)، يحتاج القارئ إلى خطة لمواصلة التعلم. هذا الفصل يوفر خارطة طريق لتطوير المهارات من خلال مصادر مجانية، أدوات عملية، ومشاريع متقدمة. الهدف هو تمكين القارئ من الانتقال من المبتدئ إلى المحترف، سواء كان هدفه تطوير أنظمة RFID، البحث الأكاديمي، أو التطبيقات التجارية.

10.1.1 لماذا مواصلة التعلم؟

- **التطور السريع**: تقنيات RFID تتطور باستمرار (مثل رقائق DESFire EV3).
- **التطبيقات المتنوعة**: من تتبع المخزون إلى إنترنت الأشياء (IoT).
- **الأمان**: فهم التشفير والهجمات (مثل التنصت) أمر حاسم.
- **الفرص المهنية**: الطلب على خبراء RFID في اللوجستيات، التجزئة، والأمن.

10.1.2 خطة التعلم الذاتي

- **مراجعة الأساسيات**: راجع الفصول السابقة (مثل هيكلية MIFARE Classic، أكواد RC522).
- **التعلم العملي**: جرب مشاريع جديدة (مثل نظام حضور باستخدام RC522).
- **استخدام الموارد المجانية**: تحميل برامج ومكتبات مجانية.
- **الانضمام إلى المجتمعات**: منتديات مثل Arduino Forum أو Reddit (r/RFID).
- **التقدم إلى مواضيع متقدمة**: مثل إدارة المفاتيح أو تكامل IoT.

10.2 أمثلة: قائمة بمواقع لتحميل برامج RFID مجانية

الوصف: قائمة بمواقع ومصادر موثوقة لتحميل برامج RFID مجانية، مع وصف لكل برنامج واستخدامه. هذه البرامج تدعم الأدوات المذكورة في الفصل الثالث (مثل NFC Tools) والتقنيات المتقدمة (مثل RC522 في الفصل السادس).

القائمة:

- **NFC Tools**:
  - **الوصف**: تطبيق لقراءة/كتابة رقائق NFC (مثل NTAG213، MIFARE Classic).
  - **الاستخدام**: قراءة UID، كتابة نصوص/روابط، حماية الرقائق بكلمات مرور.
  - **الرابط**:
    - Android: play.google.com/store/apps/details?id=com.wakdev.nfctools (#).
    - iOS: apps.apple.com/us/app/nfc-tools/id1252962749 (#).
  - **السعر**: مجاني (ميزات متقدمة مدفوعة).

- **الربط مع الفصول السابقة**: استخدم في الفصل الثالث (تمرين واجهة "Write") والفصل الخامس (كتابة "1234").
- **MTools**:
  - **الوصف**: تطبيق Android لإدارة رقائق MIFARE Classic، بما في ذلك إدارة المفاتيح.
  - **الاستخدام**: فتح قطاعات محمية، نسخ بطاقات (مع التحذير من الاستخدام غير القانوني).
  - **الرابط**: play.google.com/store/apps/details?id=studio.mightywallet.mtools (#).
  - **السعر**: مجاني (مع ميزات مدفوعة).
  - **الربط**: دعم الفصل الخامس (فتح قطاعات محمية) والفصل السادس (إدارة المفاتيح).
- **NXP TagInfo**:
  - **الوصف**: تطبيق لتحليل رقائق NFC (مثل نوع الرقاقة، التشفير).
  - **الاستخدام**: التحقق من توافق الرقائق، عرض خريطة الذاكرة.
  - **الرابط**: play.google.com/store/apps/details?id=com.nxp.taginfo (#).
  - **السعر**: مجاني.
  - **الربط**: مفيد في الفصل الثاني (فهم هيكلية الرقائق).
- **MFRC522 Library**:
  - **الوصف**: مكتبة Arduino لبرمجة RC522 (قراءة/كتابة).
  - **الاستخدام**: تنفيذ أكواد مثل DumpInfo وكتابة البيانات (راجع الفصل السادس).
  - **الرابط**: github.com/miguelbalboa/rfid (#).
  - **السعر**: مجاني.
  - **الربط**: أساسي في الفصل السادس (تمرين برمجة RC522).
- **Proxmark3 Tools**:
  - **الوصف**: أدوات مفتوحة المصدر لـ Proxmark3 لاختبار الأمان والهجمات.
  - **الاستخدام**: محاكاة هجمات (مثل استخراج المفاتيح)، تحليل الرقائق.
  - **الرابط**: github.com/Proxmark/proxmark3 (#).
  - **السعر**: مجاني.
  - **الربط**: يدعم الفصل الثامن (مناقشة الاستخدام غير القانوني).
- **LibNFC**:
  - **الوصف**: مكتبة مفتوحة المصدر لتطوير تطبيقات NFC على Linux/Windows.
  - **الاستخدام**: برمجة قارئات مثل ACR122U لتطبيقات مخصصة.
  - **الرابط**: nfc-tools.org/index.php?title=Libnfc (#).
  - **السعر**: مجاني.
  - **الربط**: مناسب للمحترفين في الفصل السادس (تقنيات متقدمة).

كيفية استخدام القائمة:

- زر المواقع المذكورة، تحقق من متطلبات النظام (مثل Android 5.0+ لـ NFC Tools).
- جرّب البرامج على رقائق تجريبية (مثل MIFARE Classic Gen1).
- راجع الفصول السابقة لفهم الاستخدام (مثل الفصل الثالث لـ NFC Tools).

صورة توضيحية:

- لقطة شاشة تُظهر صفحة تحميل NFC Tools على Google Play.
- تعليق: "مخطط 10.1: تحميل برامج RFID مجانية مثل NFC Tools."

تحدي إضافي:

- قم بتنزيل NFC Tools وNXP TagInfo، وقارن بينهما في تقرير (150-200 كلمة).
- استكشف LibNFC على Linux وجرّب قراءة UID باستخدام ACR122U.

10.3 الملحقات

10.3.1 قاموس المصطلحات

الوصف: قاموس يشرح المصطلحات التقنية المستخدمة في RFID، مع ربطها بالفصول السابقة لتعزيز الفهم.

القاموس:

- **UID (Unique Identifier)**:
  - **التعريف**: معرف فريد مكون من 4-7 بايتات يُحدد رقاقة RFID.
  - **المثال**: "A1 B2 C3 04" في MIFARE Classic.
  - **الربط**: الفصل الثاني (قراءة UID)، الفصل السادس (كود DumpInfo).
- **Sector**:
  - **التعريف**: قسم من ذاكرة رقاقة RFID يحتوي على كتل (مثل 4 كتل في MIFARE Classic).
  - **المثال**: القطاع 1 في MIFARE Classic يخزن بيانات المستخدم.
  - **الربط**: الفصل الثاني (هيكلية الرقائق)، الفصل الخامس (تغيير بيانات القطاع).
- **Encryption**:
  - **التعريف**: تشفير البيانات لحمايتها (مثل CRYPTO1 في MIFARE Classic، AES في DESFire).
  - **المثال**: مفتاح A/B في MIFARE Classic يحمي القطاعات.
  - **الربط**: الفصل الثاني (الأمان)، الفصل الثامن (حماية البيانات).
- **NDEF (NFC Data Exchange Format)**:
  - **التعريف**: تنسيق موحد لتخزين البيانات (مثل نصوص، روابط) على رقائق NFC.
  - **المثال**: كتابة URL على NTAG213.
  - **الربط**: الفصل الثاني (مخطط كتابة NDEF)، الفصل الخامس (كتابة نصوص).
- **Tag**:
  - **التعريف**: رقاقة RFID/NFC (مثل بطاقة، ملصق).
  - **المثال**: ملصق NTAG213 في متجر.
  - **الربط**: الفصل الثالث (قراءة Tags بـ NFC Tools).
- **Authentication**:
  - **التعريف**: عملية التحقق من المفتاح للوصول إلى قطاع محمي.
  - **المثال**: إدخال مفتاح "FFFFFFFFFFFF" في MTools.
  - **الربط**: الفصل الخامس (فتح قطاعات)، الفصل السادس (كود الكتابة).
- **SPI (Serial Peripheral Interface)**:
  - **التعريف**: بروتوكول اتصال بين Arduino وRC522.
  - **المثال**: توصيل MOSI، MISO، SCK.
  - **الربط**: الفصل السادس (توصيل RC522).
- **CRYPTO1**:
  - **التعريف**: خوارزمية تشفير ضعيفة تُستخدم في MIFARE Classic.
  - **المثال**: عرضة لاستخراج المفاتيح.
  - **الربط**: الفصل الثامن (الاستخدام غير القانوني).
- **DESFire**:

- **التعريف**: رقاقة RFID متقدمة تدعم AES/3DES.
- **المثال**: تُستخدم في الدفع بدون تلامس.
- **الربط**: الفصل الثاني (هيكلية DESFire).
- **IoT (Internet of Things)**:
  - **التعريف**: ربط RFID مع أنظمة متصلة بالإنترنت.
  - **المثال**: إرسال بيانات RC522 إلى السحابة.
  - **الربط**: الفصل السادس (تقنيات متقدمة).

صورة توضيحية:

- جدول يُظهر المصطلحات مع أيقونات (مثل رمز قفل لـ Encryption).
- تعليق: "مخطط 10.2: قاموس مصطلحات RFID."

10.3.2 قائمة الموارد

الوصف: قائمة بموارد لشراء الأدوات (مثل RC522، ACR122U) وتنزيل البرامج، مع روابط موثوقة.
القائمة:

- **شراء الأدوات**:
  - **Arduino Uno**:
    - **الوصف**: لوحة لبرمجة RC522.
    - **السعر**: حوالي 20-25 دولارًا.
    - **الرابط**: www.arduino.cc/en/Main/ArduinoBoardUno (#) أو www.amazon.com (#).
    - **الربط**: الفصل السادس (توصيل RC522).
  - **RC522 RFID Reader**:
    - **الوصف**: قارئ RFID بتردد 13.56 ميجاهرتز.
    - **السعر**: 5-10 دولارات.
    - **الرابط**: www.adafruit.com/product/365 (#) أو www.aliexpress.com (#).
    - **الربط**: الفصل السادس (تمرين البرمجة).
  - **ACR122U**:
    - **الوصف**: قارئ USB للكمبيوتر.
    - **السعر**: 25-30 دولارًا.
    - **الرابط**: www.acs.com.hk/en/products/3/acr122u (#) أو www.amazon.com (#).
    - **الربط**: الفصل الثالث (مقارنة القارئات).
  - **MIFARE Classic 1K Cards**:
    - **الوصف**: بطاقات RFID تجريبية.
    - **السعر**: 0.5-1 دولار لكل بطاقة.
    - **الرابط**: www.aliexpress.com (#) أو www.ebay.com (#).
    - **الربط**: الفصل الخامس (كتابة بيانات).
  - **NTAG213 Tags**:
    - **الوصف**: ملصقات NFC لتطبيقات التتبع.
    - **السعر**: 0.2-0.5 دولار لكل ملصق.
    - **الرابط**: www.nxp.com/products/nfc-tags (#).

- **الربط**: الفصل السابع (تتبع المخزون).
- **تنزيل البرامج**:
  - **Arduino IDE**:
    - **الوصف**: بيئة لبرمجة Arduino.
    - **الرابط**: www.arduino.cc/en/software (#).
    - **الربط**: الفصل السادس (أكواد RC522).
  - **NFC Tools**: (راجع قسم 10.2).
  - **MTools**: (راجع قسم 10.2).
  - **NXP TagInfo**: (راجع قسم 10.2).
- **مصادر تعليمية**:
  - **Arduino Forum**:
    - **الوصف**: مناقشات حول مشاريع RFID.
    - **الرابط**: forum.arduino.cc (#).
  - **NXP RFID Tutorials**:
    - **الوصف**: دروس حول MIFARE وNTAG.
    - **الرابط**: www.nxp.com/support (#).
  - **YouTube Channels**:
    - **الوصف**: فيديوهات تعليمية (مثل RC522 Tutorials).
    - **الرابط**: youtube.com (#) (ابحث عن "RFID Arduino Tutorial").
    - **الربط**: الفصل السادس (فيديو RC522).
  - **Reddit (r/RFID)**:
    - **الوصف**: مجتمع لمناقشة RFID.
    - **الرابط**: reddit.com/r/RFID (#).

صورة توضيحية:

- جدول يُظهر الأدوات مع أيقونات (مثل رمز بطاقة لـ MIFARE).
- تعليق: "مخطط 10.3: موارد لشراء الأدوات وتنزيل البرامج."

10.3.3 قوالب بيانات

الوصف: قوالب لبيانات RFID يمكن استخدامها في تطبيقات عملية (مثل تتبع المخزون، الحضور). القوالب جاهزة للكتابة باستخدام NFC Tools أو RC522.

القوالب:

- **قالب تتبع المخزون**:
  - **الوصف**: بيانات لتتبع منتج في مستودع.
  - **التنسيق**: NDEF (Text Record).
  - **البيانات**:

```
ProductID: PROD001
Name: Laptop XYZ
Location: Warehouse A
```

- Status: In Stock
- **الاستخدام**:
  - اكتب البيانات على NTAG213 باستخدام NFC Tools (راجع الفصل الخامس).
  - اقرأ البيانات لتحديث قاعدة بيانات (راجع الفصل السابع).
- **مثال الكتابة**:
  - في NFC Tools: "Write" → "Text" → أدخل البيانات أعلاه.
- **الربط**: الفصل السابع (سيناريو تتبع المخزون).

- **قالب الحضور**:
  - **الوصف**: بيانات لتسجيل حضور طالب.
  - **التنسيق**: NDEF (Text Record).
  - **البيانات**:

StudentID: STU123
Name: Ali Ahmed

- Class: CS101
- **الاستخدام**:
  - اكتب على MIFARE Classic باستخدام RC522 (راجع الفصل السادس).
  - استخدم كود الحضور (الفصل السابع) للتحقق.
- **مثال الكتابة**:
  - في RC522: عدّل كود الكتابة لتخزين البيانات في القطاع 1.
- **الربط**: الفصل السابع (تمرين الحضور).

- **قالب التحكم في الوصول**:
  - **الوصف**: بيانات لبطاقة دخول.
  - **التنسيق**: Raw Data.
  - **البيانات**:

UserID: USER001

- AccessLevel: Admin
- **الاستخدام**:
  - اكتب على MIFARE Classic (القطاع 2) باستخدام MTools.
  - استخدم نظام التحكم في الوصول (الفصل السابع).
- **مثال الكتابة**:
  - في MTools: "Write" → القطاع 2 → أدخل البيانات.
- **الربط**: الفصل السابع (سيناريو التحكم في الوصول).

- **قالب دفع بدون تلامس** (تجريبي):
  - **الوصف**: بيانات محاكاة للدفع (للأغراض التعليمية فقط).
  - **التنسيق**: NDEF (URL Record).
  - **البيانات**:

- PaymentURL: https://example.com/pay?user=123
- **الاستخدام**:
  - اكتب على NTAG213 باستخدام NFC Tools.
  - اقرأ باستخدام هاتف NFC لفتح الرابط.
- **تحذير**: لا تُعدّل بطاقات دفع حقيقية (راجع الفصل الثامن).
- **الربط**: الفصل الثامن (الاستخدام القانوني).

صورة توضيحية:

- جدول يُظهر القوالب مع أمثلة البيانات.
- تعليق: "مخطط 10.4: قوالب بيانات RFID جاهزة."

تحدي إضافي:

- اكتب قالب تتبع المخزون على NTAG213 باستخدام NFC Tools.
- عدّل كود RC522 لقراءة قالب الحضور وعرض البيانات.

10.4 خطة لمواصلة التعلم

الوصف: خطة عملية لتطوير مهارات RFID على مدار 6 أشهر، مع مشاريع مقترحة وربط بالفصول السابقة.
الخطة:

- **الشهر 1-2: تعزيز الأساسيات**:
  - **المهام**:
    - راجع الفصل الثاني (هيكلية الرقائق).
    - كرر تمارين الفصل الثالث (NFC Tools) والخامس (كتابة بيانات).
    - قم بتنزيل NFC Tools وNXP TagInfo (راجع 10.2).
  - **المشروع**: اكتب نصًا وعنوان URL على NTAG213 باستخدام NFC Tools.
  - **الموارد**: NFC Tools، NXP TagInfo، rfid-guide.x.ai.
- **الشهر 3-4: البرمجة والتقنيات المتقدمة**:
  - **المهام**:
    - نفّذ تمرين RC522 (الفصل السادس).
    - جرب إدارة المفاتيح باستخدام MTools.
    - تعلم أساسيات IoT (مثل إرسال بيانات إلى Blynk).
  - **المشروع**: صمم نظام حضور باستخدام RC522 (راجع الفصل السابع).
  - **الموارد**: Arduino IDE، MFRC522 Library، blynk.io (#).
- **الشهر 5-6: تطبيقات متقدمة والأخلاقيات**:
  - **المهام**:
    - نفّذ سيناريو تتبع المخزون (الفصل السابع).
    - ناقش سيناريو أخلاقي (الفصل الثامن).
    - تعلم عن DESFire وتشفير AES.
  - **المشروع**: طوّر نظام تحكم في الوصول مع قاعدة بيانات بسيطة.
  - **الموارد**: Proxmark3 Tools، NXP Tutorials، gdpr.eu (#).

مخطط ASCII لخطة التعلم:

```
+------------------------------------------+
|        خطة تعلم 6) RFID أشهر)          |
+------------------------------------------+
| [الشهر 1-2: الأساسيات]              |
|  | مراجعة الفصل 2، 3، 5             |
|  | مشروع: كتابة NDEF على NTAG213          |
|  v                                   |
| [الشهر 3-4: البرمجة]               |
|  | تمرين RC522 (الفصل 6)              |
|  | مشروع: نظام حضور                 |
|  v                                   |
| [الشهر 5-6: التطبيقات]              |
|  | سيناريو تتبع، مناقشة أخلاقية       |
|  | مشروع: تحكم في الوصول             |
+------------------------------------------+
```

- **الصورة في الكتاب**: رسم تدفقي ملون يوضح الخطة (مخطط 10.5: خطة التعلم).

تحدي إضافي:

- أنشئ جدولًا زمنيًا أسبوعيًا للشهر الأول.
- انضم إلى Arduino Forum وشارك مشروعك.

10.5 مشاريع مقترحة للتعلم المتقدم

- **نظام مكافحة السرقة:**
  - **الوصف**: استخدم RC522 لتتبع الأصول في متجر.
  - **الأدوات**: RC522، Arduino، جرس تنبيه.
  - **الربط**: الفصل السابع (تتبع المخزون).
- **قفل ذكي:**
  - **الوصف**: قفل باب يفتح فقط لبطاقات مُصرح لها.
  - **الأدوات**: RC522، Arduino، مرحل.
  - **الربط**: الفصل السابع (التحكم في الوصول).
- **تطبيق IoT:**
  - **الوصف**: إرسال بيانات RFID إلى السحابة (مثل Firebase).
  - **الأدوات**: RC522، ESP32، Firebase.
  - **الربط**: الفصل السادس (تقنيات متقدمة).
- **اختبار الأمان:**
  - **الوصف**: محاكاة هجوم استخراج مفتاح على MIFARE Classic.
  - **الأدوات**: Proxmark3، MTools.
  - **الربط**: الفصل الثامن (الاستخدام غير القانوني).

صورة توضيحية:

- رسم يُظهر مشاريع (مثل قفل ذكي مع رمز RFID).

- تعليق: "مخطط 10.6: مشاريع RFID متقدمة."

ملخص الفصل

- مواصلة التعلم تتطلب مراجعة الأساسيات، البرمجة، والتطبيقات العملية.
- الموارد المجانية (مثل NFC Tools، MFRC522 Library) تُسهل التعلم.
- قاموس المصطلحات يُبسط المفاهيم التقنية.
- قوالب البيانات تُسرّع تصميم الأنظمة.
- خطة التعلم تُنظم التقدم من المبتدئ إلى المحترف.

أسئلة مراجعة

- ما أهمية مواصلة التعلم في RFID؟
- كيف تُساعد برامج مثل NFC Tools المبتدئين؟
- ما فائدة قاموس المصطلحات؟
- كيف تُستخدم قوالب البيانات في التطبيقات؟
- ما المشاريع المناسبة لتعلم RFID المتقدم؟

موارد إضافية

- **فيديوهات**:
  - "تعلم RFID من الصفر" (youtube.com/rfid-learning (#)).
  - "مشاريع RFID متقدمة" (youtube.com/rfid-projects (#)).
- **مواقع**: rfid-guide.x.ai، nfc-tools.org (#).
- **مجتمعات**: Arduino Forum، Reddit (r/RFID).